



M86 MailMarshal SMTP

# USER GUIDE

Software Version: 6.8.4

# **M86 MAILMARSHAL SMTP USER GUIDE**

© 2010 M86 Security  
All rights reserved.

Published October 2010 for software release 6.8.4

No part of this Documentation may be reproduced or transmitted in any form or by any means, including but without derogation of the foregoing, electronic or mechanical means, photocopying, recording or any information storage and retrieval system, without the prior permission in writing of M86 Security.

This Documentation is provided “as is” and there are no warranties or representations made by M86 Security, either express, implied, or statutory, with respect to it, including warranties or conditions of title, quality, non-infringement, merchantability, quality or fitness for a particular purpose, nor are there any warranties created by course of dealing, course of performance, or trade usage. M86 Security does not warrant that this Documentation will meet your needs or be free from errors. In no event will M86 Security be liable for any form of loss or damage of whatsoever kind (whether arising in contract, tort, by statute or otherwise), including, but without limiting the generality of the foregoing, direct, damages at common law, repudiatory damages indirect, special, idiosyncratic or consequential damages or loss, loss of anticipated profits, loss of business opportunity or loss of contracts by you or any third party or claims or demands against you by any third party or other like economic loss in connection with or arising out of your use and/or possession of this Documentation.

M86 MailMarshal SMTP is the registered trademark of M86 Security. Other product names mentioned in this Documentation may be trademarks or registered trademarks of their respective companies.

---

# Contents

About This Book and the Library .....	xiii
Conventions .....	xiv

## Chapter 1

<b>Introduction.....</b>	<b>1</b>
What Is MailMarshal SMTP? .....	1
What Does MailMarshal SMTP Provide? .....	3
How MailMarshal SMTP Helps You .....	4
Filters Email at the Gateway .....	5
Delivers Layered Spam Protection .....	5
Protects Against Existing and Emerging Threats .....	5
Provides Unparalleled Performance .....	6
Includes Easy-to-Use Interfaces .....	6
How MailMarshal SMTP Works .....	6
Understanding What MailMarshal SMTP Does .....	7
Configuring MailMarshal SMTP .....	9
Monitoring and Reporting .....	10
MailMarshal SMTP Node Appliance .....	11
MailMarshal SMTP and MailMarshal Exchange .....	11

## Chapter 2

<b>Planning Your MailMarshal SMTP Installation.....</b>	<b>13</b>
Planning Checklist .....	13
Understanding MailMarshal SMTP Components .....	15
MailMarshal SMTP Components .....	17
Other Software and Services .....	18
Understanding Installation Scenarios .....	19
Standalone Installation .....	19
Array Installation .....	24

Hardware and Software Requirements .....	26
Standalone Installation Requirements .....	26
Array Installation Requirements .....	29
Web Components Requirements .....	32
Configurator or Console User Interface Requirements .....	33
Reports User Interface Requirements .....	34
Database Software Considerations .....	35
Understanding MailMarshal SMTP Folder Locations .....	37
Supported Antivirus Software .....	38
Collecting Information for Installation .....	39

### **Chapter 3**

<b>Installing and Configuring MailMarshal SMTP .....</b>	<b>43</b>
Installation Checklist .....	43
Installing Prerequisite Software .....	45
Installing MailMarshal SMTP on a Standalone Server .....	46
Installing MailMarshal SMTP as an Array .....	48
Installing a MailMarshal SMTP Array Manager .....	49
Installing a MailMarshal SMTP Server .....	52
Running the Configuration Wizard .....	56
Configuring Email Routing .....	61
Creating Directory Connectors .....	62
Configuring Antivirus Scanning .....	65
Excluding Working Folders From Virus Scanning .....	65
Configuring MailMarshal SMTP to Use an Antivirus Product .....	67
Installing MailMarshal SMTP Reports .....	69
Installing and Customizing Web Components .....	70
Installing the MailMarshal SMTP Web Components .....	71
Customizing the Web Components .....	74
Installing Additional User Interfaces .....	75

---

Upgrading MailMarshal SMTP .....	76
Upgrading from MailMarshal SMTP Version 6.4.5 or Above .....	76
Upgrading from Other Versions of MailMarshal SMTP .....	80
Uninstalling MailMarshal SMTP .....	81

## **Chapter 4**

<b>Understanding MailMarshal SMTP Interfaces.....</b>	<b>85</b>
Understanding the Configurator .....	86
Working With the Getting Started and Common Tasks Pages .....	87
Working With Menu and Detail Items .....	88
Working With Properties Configuration .....	88
Committing Configuration .....	89
Understanding the Console .....	90
Understanding the Web Console .....	92
Understanding the Reports Console .....	93
Understanding the Spam Quarantine Management Website .....	94
Understanding Other Tools .....	95

## **Chapter 5**

<b>Implementing Your Email Content Security Policy.....</b>	<b>97</b>
Configuring Email Content Security .....	97
Stopping Spam .....	98
Spam Configuration and Rules .....	98
Configuring SpamProfiler .....	101
Configuring SpamCensor and SpamProfiler Updates .....	102
Stopping Viruses .....	105
How MailMarshal SMTP Uses Virus Scanners .....	105
Virus and Threats Policy and Rules .....	107
Best Practices .....	108
Viewing Virus Scanner Properties .....	109
Preventing Relaying .....	109

Controlling Who Can Send Email Through Your Server .....	111
Reputation Services and DNS Blacklists .....	112
PTR Lookups .....	114
Blocked Hosts .....	115
Authentication by Account .....	116
Preventing Malicious Email Attacks .....	116
Understanding Denial of Service Attack Prevention .....	117
Preventing Denial of Service Attacks .....	118
Enabling and Disabling DoS Attack Prevention .....	119
Understanding Directory Harvest Attack Prevention .....	120
Preventing Directory Harvest Attacks .....	122
Enabling and Disabling Directory Harvest Attack Prevention .....	123
Filtering Messages and Attachments .....	124

## **Chapter 6**

<b>Understanding Email Policy, Policy Groups, and Rules .....</b>	<b>127</b>
Understanding Policy Groups .....	127
Understanding Rules .....	129
Receiver Rules .....	129
Standard Rules .....	129
Creating Rules .....	129
Understanding User Matching .....	131
Understanding Rule Conditions .....	133
Rule Conditions for Standard Rules .....	134
Rule Conditions for Receiver Rules .....	155
Understanding Rule Actions .....	159
Rule Actions for Standard Rules .....	160
Rule Actions for Receiver Rules .....	169
Understanding the Order of Evaluation .....	170
Adjusting the Order of Evaluation of Policy Groups .....	171
Adjusting the Order of Evaluation of Rules .....	171
Viewing Email Policy .....	173

---

<b>Chapter 7</b>	
<b>Understanding Email Policy Elements .....</b>	<b>175</b>
Configuring Connectors .....	177
Configuring User Groups .....	179
Creating and Populating User Groups .....	179
Moving and Copying Users and Groups .....	183
Identifying Email Text Content Using TextCensor Scripts .....	184
Creating Scripts .....	184
Editing Scripts .....	187
Duplicating Scripts .....	188
Script and Item Weighting .....	188
Item Syntax .....	190
Importing Scripts .....	191
Exporting Scripts .....	192
TextCensor Best Practices .....	192
Testing Scripts .....	194
Notifying Users with Message Templates and Message Stamps .....	194
Message Templates .....	195
Creating a Message Template .....	196
Creating Digest Templates .....	198
Editing Templates .....	201
Duplicating Templates .....	201
Deleting Templates .....	202
Working with Message Stamps .....	202
Using Variables .....	204
Date Formatting .....	210
Using Virus Scanning .....	212
Using Email Folders and Message Classifications .....	212
Working with Message Classifications .....	213
Working with Folders .....	215
Creating Folders .....	216
Editing Folders .....	217

---

Header Matching and Rewriting .....	218
Changing and Adding Headers with the Receiver .....	218
Using Rules to Find Headers .....	219
Using Rules to Change Headers .....	219
Using the Header Rewrite Wizard .....	220
Extending Functionality Using External Commands .....	225
Configuring Reputation Services .....	228
<b>Chapter 8</b>	
<b>Monitoring Email Flow .....</b>	<b>229</b>
Using the MailMarshal SMTP Console .....	231
Connecting to MailMarshal SMTP Using the Console .....	231
Connecting to MailMarshal SMTP Using the Web Console .....	232
Viewing Server Statistics .....	232
Deleting and Retrying Queued Messages .....	234
Viewing Folders and Folder Contents .....	235
Working With Email Messages .....	236
Viewing Email History .....	243
Searching Folders and Email History .....	244
Viewing Alert History .....	245
Setting Console Security .....	246
Viewing Event History .....	250
Finding Events .....	251
Viewing News From M86 Security .....	253
Using Windows Tools .....	254
Event Log .....	254
Performance Monitor .....	254
Using MailMarshal SMTP Text Logs .....	255



---

## Chapter 9

### **Managing MailMarshal SMTP Configuration..... 257**

Managing Your MailMarshal SMTP Licenses .....	257
Reviewing Installed Licenses .....	258
Requesting a New License Key .....	259
Entering a License Key .....	259
Backing Up and Restoring the Configuration .....	260
Backing Up the Configuration .....	261
Restoring the Configuration .....	263
Configuring Local Domains .....	264
Changing Local Domains Information .....	265
Configuring Routes .....	267
Editing Routing Table Information .....	268
Configuring Relaying .....	273
Editing Relay Table Information .....	273
Configuring Delivery Options .....	275
Configuring Default Delivery Options .....	276
Configuring Delivery Options For A Specific Server .....	277
Setting Up Accounts .....	278
Creating Accounts .....	279
Editing Existing Accounts .....	280
Deleting Accounts .....	280
Configuring Email Batching .....	281
Configuring Manager Security .....	281
Managing Array Nodes .....	282
Managing Node Services .....	282
Adding and Deleting Nodes .....	283
Joining a Node to an Array .....	285
Customizing Settings for Nodes .....	286
Managing Appliance Nodes .....	287
Understanding Secure Email Communications .....	288

Securing Email Communications .....	289
Working with Certificates .....	289
Securing Inbound Communications .....	290
Securing Outbound Communications .....	291
Setting Anti-Virus Update Options .....	292
Setting Advanced Options .....	292
MailMarshal Properties - Advanced .....	292
Setting Node Properties - Advanced .....	293
Working with Array Communications .....	294
Changing Folder Locations .....	297
Using the Group File Import Tool .....	298
Using the Configuration Export Tool .....	300

## **Chapter 10**

### **Delegating Spam and Quarantine Management..... 303**

Setting Up Console Access .....	304
Setting Up Spam Quarantine Management Features .....	304
Spam Quarantine Management Windows .....	305
Setting Up Folders and Templates .....	307
Setting Up Message Digests .....	308
Setting Up Rules .....	310
Setting Up Spam Quarantine Management for Other Folders .....	311
Using the Message Release External Command .....	312

## **Chapter 11**

### **Reporting on MailMarshal SMTP Activity..... 317**

Data Retention and Grouping .....	318
Configuring Data Retention .....	318
Configuring Reporting Groups .....	319
Connecting to the Database .....	320

---

Generating Reports .....	320
Available Reports .....	321
Entering Report Parameters .....	321
Available Parameters .....	323
Navigating the Report Window .....	323
Exporting Reports .....	324

## **Appendix A**

### **Wildcards and Regular Expressions 329**

Wildcard Characters .....	329
Regular Expressions .....	331
Shortcuts .....	331
Reserved Characters .....	332
Examples .....	334
Map Files .....	335

## **Appendix B**

### **Third Party Extensions 337**

Image Analyzer .....	337
Why Would I Use Image Analyzer? .....	338
What Results Can I Expect From Image Analyzer? .....	339
How Does Image Analyzer Address the Issues? .....	339
Virus Scanning Software .....	340
Anti-Spyware Scanners .....	340

### **Glossary 341**

### **Index 347**



---

# ABOUT THIS BOOK AND THE LIBRARY

The *User Guide* provides conceptual information about MailMarshal SMTP. This book defines terminology and various related concepts.

## Intended Audience

This book provides information for individuals responsible for understanding MailMarshal SMTP concepts and for individuals managing MailMarshal SMTP installations.

## Other Information in the Library

The library provides the following information resources:

### *Evaluation Guide*

Provides general information about the product and guides you through the trial and evaluation process.

### *User Guide*

Provides conceptual information and detailed planning and installation information about MailMarshal SMTP. This book also provides an overview of the MailMarshal SMTP user interfaces and the Help.

### *Appliance Quick Start Guide*

Provides an overview of the steps required to set up a MailMarshal Appliance installation.

### *Appliance Administrator Guide*

Provides detailed information about the options available through the web based interface for the MailMarshal Node Appliance (NEWS interface).

### *Help*

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

---

# CONVENTIONS

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
<b>Bold</b>	<ul style="list-style-type: none"><li>• <i>Window and menu items</i></li><li>• <i>Technical terms, when introduced</i></li></ul>
<i>Italics</i>	<ul style="list-style-type: none"><li>• <i>Book and CD-ROM titles</i></li><li>• <i>Variable names and values</i></li><li>• <i>Emphasized words</i></li></ul>
Fixed Font	<ul style="list-style-type: none"><li>• <i>File and folder names</i></li><li>• <i>Commands and code examples</i></li><li>• <i>Text you must type</i></li><li>• <i>Text (output) displayed in the command-line interface</i></li></ul>
Brackets, such as [ <i>value</i> ]	<ul style="list-style-type: none"><li>• <i>Optional parameters of a command</i></li></ul>
Braces, such as { <i>value</i> }	<ul style="list-style-type: none"><li>• <i>Required parameters of a command</i></li></ul>
Logical OR, such as <i>value1</i>   <i>value2</i>	<ul style="list-style-type: none"><li>• <i>Exclusive parameters. Choose one parameter.</i></li></ul>

---

# Chapter 1

## Introduction

Email is an essential communication tool, but it also creates serious productivity and security issues. Email offers an entry point in your network for spam and other undesired non-business content, such as malicious code, large file attachments that consume valuable disk space, phishing attempts, information and identity theft attacks, and other damaging content and activity.

In addition, email can become a conduit for proprietary data and confidential information to leave the company. Spam, email viruses, malicious code, liability issues, and declining employee productivity are all risks associated with email.

Spam commonly accounts for more than half of the email companies receive. Email viruses, Trojan horses, and other malicious files can cause millions of dollars in damage in just a matter of hours. Reports of companies forced into legal action because of staff misuse of email are becoming commonplace.

Email remains the lifeblood of modern business communication, but the damages email can cause become more costly each year.

## WHAT IS MAILMARSHAL SMTP?

MailMarshal SMTP is a fast, easy-to-use email content security solution that ensures a safe and productive working environment by enforcing your Acceptable Use Policy and protecting against spam, viruses, and other undesirable content.

MailMarshal SMTP features a layered security approach to dramatically reduce spam and protect your network. This approach delivers a greater than 97% spam detection rate with less than 0.001% false positives. The product performs up to four times faster than other available products.

Key elements of the MailMarshal SMTP anti-spam solution include:

- **SpamProfiler**, an antispam pre-filter that can reject spam email without unpacking and full processing.
- **SpamCensor**, an advanced antispam engine that can filter most spam before it enters your network.
- **SpamBotCensor**, an optimized application of SpamCensor that can block spam generated by botnets with even greater efficiency.
- **Blended Threats Module**, a real-time identification system for threat URLs contained in email.
- **Automatic updates** for SpamProfiler and SpamCensor responding to the latest trends in Spam.
- **Zero Day updates** protecting you from significant spam and malware events.
- **URLCensor**, to reject email based on blacklisted URLs embedded in messages.
- **TextCensor**, to analyze and filter inbound and outbound messages based on language content.

MailMarshal SMTP is a gateway product that can be used with any internal company email system, including Microsoft Exchange, Novell GroupWise, Lotus Domino, Sendmail, and Linux email servers. MailMarshal SMTP provides your company with the layered security solution you need to manage email content, fight spam, and transparently enforce your email Acceptable Use Policy.

Many organizations today have created policies and guidelines for the appropriate use of email, and employee education programs to deal with the torrent of spam and viruses. MailMarshal SMTP can help your company automatically apply email policy and security at the gateway, so you can once again use email safely, securely and productively.



# WHAT DOES MAILMARSHAL SMTP PROVIDE?

As a gateway content security solution, MailMarshal SMTP protects your network and your organization. MailMarshal SMTP enforces your Acceptable Use Policy to protect against spam, viruses, gateway email attacks, and other undesirable consequences of using email.

Easily supporting enterprises with tens of thousands of users, MailMarshal SMTP is by far the most powerful, feature rich email content security solution available.

MailMarshal SMTP scans the content of inbound and outbound email messages, including the headers, message body, and attachments. MailMarshal can detect many conditions, such as:

- Attempted message delivery from a blacklisted server
- Presence of a virus (using one or more supported virus scanners)
- Presence of particular phrases in header, message, or attachment
- Size or type of attachments
- Presence of blacklisted URLs in header, message, or attachment

The product can also respond to messages that violate your Acceptable Use Policy, by taking actions such as:

- Refusing receipt of a message from a remote server
- Quarantining a message for later review by administrators or users
- Deleting a message
- Redirecting a message
- Archiving a message for future reference

MailMarshal SMTP provides email administrators with granular control of policies and the ability to delegate email monitoring and control to other personnel. MailMarshal SMTP provides the following user interfaces to meet the needs of a variety of administrators and your email recipients:

**Configurator**

For email security administrators to configure the product and establish email policy.

**Console**

For email administrators and helpdesk personnel to monitor and control product activity. Also available as a Web based application.

**Reports**

For auditors and email administrators to report on spam-blocking effectiveness and overall email use.

**Spam Quarantine Management Website**

For email recipients to verify quarantined email and customize spam blocking for their own email addresses.

## HOW MAILMARSHAL SMTP HELPS YOU

Unmonitored email presents both financial and legal dangers to a company. For example, spam represents a dramatic financial threat in terms of the cost of storage, bandwidth, and wasted employee time. Virus infection and malicious code can be costly in employee time, repair time, and lost data. Inappropriate and offensive email content wastes time and is a potential liability.

Using MailMarshal SMTP, your company can earn a significant ROI as you secure your network, protect corporate assets, reduce the potential for corporate liability, and improve workplace productivity.

## **Filters Email at the Gateway**

MailMarshal SMTP analyzes email content and attachments entering your network to deliver a greater than 97% spam detection rate with less than 0.001% false positives. MailMarshal SMTP protects your network and resources by reducing spam and eliminating other undesirable content before it enters your network. By scanning for viruses and detecting and preventing gateway attacks, MailMarshal SMTP helps ensure network availability for business purposes.

## **Delivers Layered Spam Protection**

MailMarshal SMTP provides a multi-layered approach to email security, pioneering the latest technologies to protect your business from spam, gateway attacks, viruses, phishing attempts, and known malicious URLs embedded in email. Using proprietary SpamProfiler, SpamCensor, Blended Threats Module, URLCensor, and TextCensor technology to detect offensive and undesired content, MailMarshal SMTP responds to these emails with the actions you define to help enforce your email Acceptable Use Policy.

## **Protects Against Existing and Emerging Threats**

MailMarshal SMTP integrates a wide variety of anti-spam and anti-threat technology to protect against known threats, as well as regular updates to meet emerging threats. The M86 Security Labs team continually updates threat detection algorithms to detect new forms of spam, mass mailing worms, and phishing scams. MailMarshal SMTP can automatically download these updates to keep your protection levels current. The M86 Security Labs team also publishes Zero Day updates to meet specific threats. The MailMarshal SMTP Blended Threats module and IP Reputation Service provide real-time updates of proprietary databases of malware URLs and spam-related email servers.

## **Provides Unparalleled Performance**

In parallel with superior spam detection and multi-layered threat protection, MailMarshal SMTP provides exceptional performance, operating up to four times faster than other spam-detection products. Scalable configurations allow MailMarshal SMTP to work for small or large organizations and to grow as your company does. This hard-working product lets you configure for redundancy to meet demanding SLAs and operate MailMarshal SMTP in geographically separate locations from a central console.

## **Includes Easy-to-Use Interfaces**

MailMarshal SMTP is easy to evaluate, install, and use. Default settings provide excellent anti-spam performance “out of the box.” The Configurator provides an intuitive interface that allows policy administrators to refine the rules MailMarshal SMTP uses to evaluate and reject or deliver email. The Console allows email administrators to monitor product effectiveness using a local client or a Web-based interface. Auditors and managers can easily produce MailMarshal SMTP reports using the Reports Console. A Web-based management console allows email users to review quarantined email, and establish and manage personal rules for acceptable and unacceptable email. These user interfaces allow various users to easily access the information they need about the MailMarshal SMTP solution.

## **HOW MAILMARSHAL SMTP WORKS**

MailMarshal SMTP is a server-based Simple Mail Transfer Protocol (SMTP) email content scanning product that is easy to install in new or existing networks with other gateway applications. It complements and is compatible with traditional Internet firewalls, SMTP mail servers, antivirus scanners, and other security applications.

MailMarshal SMTP includes several components including the Array Manager, one or more email processing servers, a Microsoft SQL Server database, and optional management websites. Small organizations can install the components on a single computer, that can also act as the local SMTP/POP3 email server. Large organizations can install the components across several computers. Enterprises can manage a distributed array of email processing servers with a single Array Manager computer.

MailMarshal SMTP provides a number of user interfaces, including the Configurator, Console, Web Console, Spam Quarantine Management site, and Reports. The Configurator lets security policy administrators set email policy for the entire organization from a central console. You can install additional user interfaces on other computers throughout the network as needed.

## **Understanding What MailMarshal SMTP Does**

The MailMarshal installation functions as the email gateway of an organization. All inbound and outbound email passes through the MailMarshal Server. You can use multiple MailMarshal Servers to provide multiple gateways or to add bandwidth and redundancy to a single gateway.

Each MailMarshal Server runs several component services, including the Receiver, Engine, and Sender services.

Receiver Functions	Engine Functions	Sender Functions
<ul style="list-style-type: none"> <li>• <i>Inbound TLS</i></li> <li>• <i>SMTP Authentication</i></li> <li>• <i>Blocked Hosts</i></li> <li>• <i>Relaying Tables</i></li> <li>• <i>DoS Protection</i></li> <li>• <i>DHA Protection</i></li> <li>• <i>Reputation Services (DNS Blacklists)</i></li> <li>• <i>Global Header Rewriting</i></li> <li>• <i>Receiver Rules</i></li> <li>• <i>SPF Evaluation</i></li> <li>• <i>SpamProfiler rejection</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Standard Rules</i></li> <li>• <i>Malware Scanning</i></li> <li>• <i>SpamBotCensor</i></li> <li>• <i>SpamProfiler and SpamCensor quarantining</i></li> <li>• <i>SpamCensor advanced usage (spam types)</i></li> <li>• <i>NDRCensor</i></li> <li>• <i>Blended Threats Module</i></li> <li>• <i>Message Archiving</i></li> <li>• <i>Route Message To Host</i></li> <li>• <i>Message Parking</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Domain Routing Tables</i></li> <li>• <i>Outbound TLS</i></li> <li>• <i>SMTP Authentication</i></li> </ul>

All inbound and outbound email enters the MailMarshal Server at the Receiver. MailMarshal SMTP can apply SpamProfiler checks and Receiver rules to messages. Receiver blocking options offer powerful protection because they allow you to refuse incoming email based on criteria such as email not addressed to a recipient in your organization. Receiver rules that block email this way conserve resources for other legitimate email.

Next, the MailMarshal Engine unpacks each email, expanding any attached archive or compressed files. The Engine then checks each component against the email policy (rules) you have enabled, including SpamCensor scripts, URLEncensor, TextCensor scripts, and any other rules you have enabled. You can alter the effects of MailMarshal SMTP rules by changing the rule order and by changing specific characteristics of the rule.

MailMarshal SMTP also scans email for viruses using antivirus scanning software. MailMarshal SMTP supports several scanners with high-throughput interfaces. The product can also use any antivirus scanner that provides a scanning response in the correct format (most antivirus scanners do).

After the MailMarshal Engine evaluates each email component against the rules, it determines whether to accept, modify, or quarantine the email.

- Accepted email is passed to the MailMarshal SMTP Sender, which then delivers it to the appropriate recipients.
- Modified email may be delivered to recipients with attachments removed.
- Virus-laden email is quarantined, or can optionally be cleaned and delivered.

MailMarshal SMTP can also notify administrators of specific actions or notify end-users of quarantined email. You can associate the appropriate rule action when you create or modify rules.

## Configuring MailMarshal SMTP

You configure MailMarshal SMTP rules and settings using the Configurator interface, connected to the MailMarshal Array Manager. The Array Manager coordinates the activity of all other MailMarshal Servers in the array and connects with the user interfaces, optional Web server, and the database.

The initial configuration settings allow MailMarshal SMTP to act as the email gateway of an organization. You can enforce a wide variety of Acceptable Usage Policies by customizing the way MailMarshal SMTP processes email connections, content, and attachments.

## Monitoring and Reporting

MailMarshal SMTP provides additional user interfaces for monitoring and daily email administration. The Console features the Dashboard to summarize MailMarshal SMTP activity and server health at a glance. Using the Console, email administrators can review email processing history for a message and view and release any quarantined message.

The administrator can grant other users access to specific Console functions or specific quarantine folders. Using this feature, the administrator can delegate basic tasks to help desk or departmental personnel.

MailMarshal SMTP also offers a Web version of the Console to allow remote access to the Console capabilities.

Email users can review and manage suspected spam and other quarantined email using daily email digests and the Spam Quarantine Management Web-based console. This console is a Web application you can easily deploy on your intranet Web server running Microsoft Internet Information Services (IIS).

Administrators and managers can generate reports on MailMarshal SMTP activity using either of two applications:

- MailMarshal SMTP Reports uses the Crystal Reports engine to produce versatile and detailed reports and graphs. This is a MMC application that can be installed on one or more workstations.
- Marshal Reporting Console uses SQL Server Reporting Services to produce reports. This is a server application with a website interface. Marshal Reporting Console can deliver reports by web view, email, FTP, or local network files, and can schedule automatic delivery of reports.

MailMarshal SMTP Reports is included in the main MailMarshal SMTP installation package. Marshal Reporting Console is provided as a separate package from M86 Security. Both applications are available to all MailMarshal SMTP customers.



# MAILMARSHAL SMTP NODE APPLIANCE

MailMarshal SMTP is available as an appliance solution. In this solution the email processing servers (“processing nodes”) are hardware appliances. The Array Manager and user interfaces are identical to those supplied with the software solution.

The MailMarshal Appliance solution differs from the software solution in the following features:

- Virus scanning is provided using McAfee for Marshal only.
- The MailMarshal POP3 service is not available. Accounts can be used for authentication only.
- For resiliency, the minimum required free disk space is substantially greater.

This Guide provides information about both the software solution and the hardware appliance solution. Differences are noted throughout this Guide and the Help. Additional information about the Appliance is available in the *Appliance Quick Start Guide* and the *Appliance Administrator Guide*.

## MAILMARSHAL SMTP AND MAILMARSHAL EXCHANGE

MailMarshal SMTP is a gateway solution that applies email content security for email inbound from or outbound to the Internet. MailMarshal Exchange provides email content security for email sent or received *internally* when you use Microsoft Exchange as your email server. MailMarshal Exchange lets you scan internal email and apply your internal Acceptable Use Policy.

If you require both internal and external email content security, you can use both products. With adequate computer resources, MailMarshal SMTP and MailMarshal Exchange can run on a single computer.

For more information about MailMarshal Exchange, see the *User Guide* for MailMarshal Exchange.

---

## Chapter 2

# Planning Your MailMarshal SMTP Installation

When planning to install MailMarshal SMTP, you should understand how MailMarshal SMTP manages email and the recommended installation scenarios based on your needs. This chapter provides information about these concepts and provides hardware requirements, software requirements, and planning checklists to help you through the planning process.

## PLANNING CHECKLIST

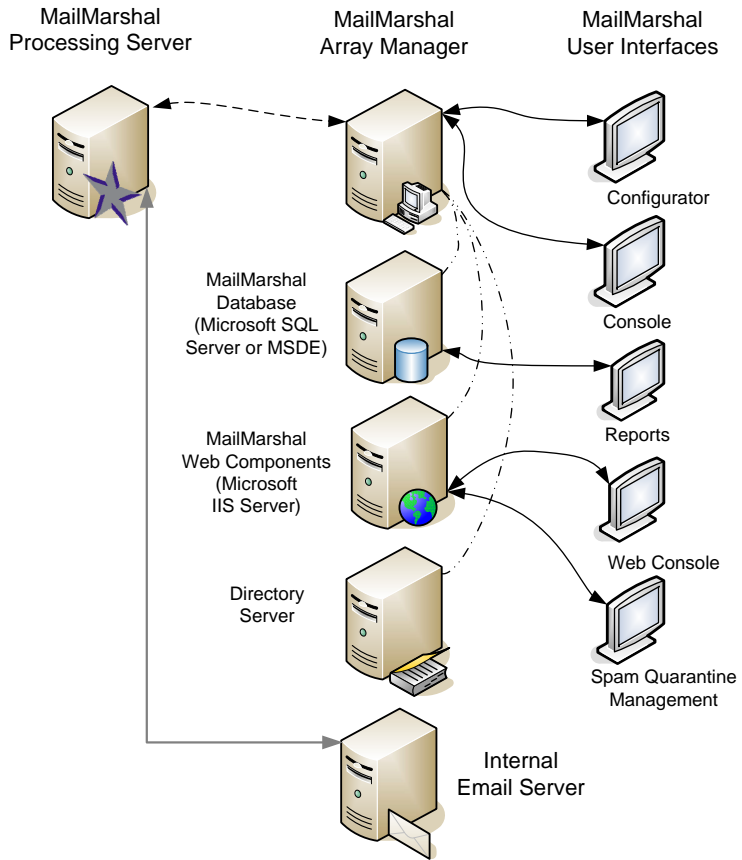
Plan your MailMarshal SMTP installation by reading the following sections and completing the following checklist:

<input checked="" type="checkbox"/>	Step	See Section
<input type="checkbox"/>	1. Learn about important MailMarshal SMTP concepts.	"Understanding MailMarshal SMTP Components" on page 15.
<input type="checkbox"/>	2. Choose a <i>standalone</i> or <i>array</i> installation.	"Understanding Installation Scenarios" on page 19.
<input type="checkbox"/>	3. <b>If you selected a standalone installation</b> , choose the appropriate configuration for your environment.	"Standalone Installation" on page 19.
<input type="checkbox"/>	4. <b>If you selected an array installation</b> , determine the number and location for the MailMarshal SMTP Servers and Array Manager components.	"Array Installation" on page 24.

<input checked="" type="checkbox"/>	Step	See Section
<input type="checkbox"/>	5. Ensure the computers meet the hardware and software requirements.	"Standalone Installation Requirements" on page 26 or "Array Installation Requirements" on page 29
<input type="checkbox"/>	6. Determine whether to use Microsoft SQL Server or SQL Express.	"Database Software Considerations" on page 35.
<input type="checkbox"/>	7. Decide where to install the MailMarshal SMTP folders.	"Understanding MailMarshal SMTP Folder Locations" on page 37.
<input type="checkbox"/>	8. Choose the antivirus software to use with MailMarshal SMTP.	"Supported Antivirus Software" on page 38.
<input type="checkbox"/>	9. Collect installation information about your email environment.	"Collecting Information for Installation" on page 39.

# UNDERSTANDING MAILMARSHAL SMTP COMPONENTS

MailMarshal SMTP consists of several software components, which you can install on different computers in your network. These components can be installed in a variety of configurations to suit any size organization from small businesses to distributed enterprises. While the components are shown on separate computers in the following figure, in lower volume scenarios you can install all components on a single computer.



## MailMarshal SMTP Components

MailMarshal SMTP includes the following components:

### Server

Accepts incoming email (Receiver), applies policy in the form of rules (Engine), and forwards email to your email server or to the recipient (Sender). You can use one or more MailMarshal SMTP Servers in your installation.



**Note:** In a MailMarshal SMTP **Appliance** installation, the server(s) are pre-configured hardware appliances.

### Array Manager

Manages an **array** of MailMarshal SMTP email processing servers. The Array Manager connects to the email processing servers and to the database, hosted using Microsoft SQL Server or SQL Express. For more information, see “Other Software and Services” on page 18.

### Configurator

User interface allowing email policy Administrators to define policy (rules) and configure MailMarshal SMTP.

### Console

User interface allowing email Administrators to manage and monitor undelivered or filtered email.

### Reports

User interface allowing administrators or auditors to prepare email management reports.

### Web Console

Web based interface used by roaming email Administrators just as they would use the Console.

### Spam Quarantine Management Website

Web based interface used by email users to view and manage quarantined email.

To operate properly, MailMarshal SMTP requires an Array Manager, at least one email processing Server, a database, a Configurator, and a Console. You can optionally install Reports and Web Components if you plan to use the additional features these components offer.

## Other Software and Services

In addition, MailMarshal SMTP may require the following software and network services:

### **Microsoft SQL Server or SQL Express**

The MailMarshal SMTP database stores configuration data and log information. If your email volume permits, you can use the free SQL Express. If your email volume is higher, use Microsoft SQL Server. If possible, install the database software and the MailMarshal SMTP Array Manager on the same computer. For more information, see “Array Installation Requirements” on page 29 and “Database Software Considerations” on page 35.

### **Directory Server**

If you want to import existing users and groups from your directory service for use in applying email Acceptable Use Policy, the MailMarshal SMTP Array Manager must be able to connect with your directory server. MailMarshal SMTP can connect with Microsoft Active Directory and most LDAP compliant directories, such as Novell NDS/eDirectory, Microsoft Exchange Server 5.5, Netscape Directory Server, and Lotus Domino.

### **Microsoft Internet Information Services (Microsoft IIS)**

If you want to offer the Web Console and end-user Spam Quarantine Management Website, install the MailMarshal SMTP Web Components on a server with Microsoft IIS and ASP.NET 3.5 SP1 installed.



# UNDERSTANDING INSTALLATION SCENARIOS

While you can configure MailMarshal SMTP to run in many environments, there are two basic configurations to consider, based on the number of users and your typical email volume:

- Standalone, or basic installation (several variations available)
- Array installation

The **standalone installation** scenario is appropriate for small to mid-size organizations with a lower volume of email. This option allows smaller organizations to gain all the benefits of using MailMarshal SMTP to reduce email volume and block annoying and costly spam.

The **array installation** is appropriate for larger, distributed organizations where email volume is high, or where use of a Demilitarized Zone (DMZ) is necessary. This option provides all the security and efficiency options larger organizations require.

For more information about determining your configuration needs, see the White Paper titled “MailMarshal SMTP Sizing Guide” at [www.m86security.com](http://www.m86security.com), or contact your Technical Support representative.

## Standalone Installation

For small to medium-sized organizations, a standalone installation provides convenience and value. In a standalone installation, you install all the MailMarshal SMTP components as well as the SQL Express or Microsoft SQL Server database on a single computer.

You can install the MailMarshal SMTP Configurator, Console, or Reports user interfaces on one or more computers in the local network.

To use the MailMarshal SMTP Web Console or enable your users to manage quarantined email with the Spam Quarantine Management Website, install the MailMarshal SMTP Web Components on a Microsoft IIS Server.

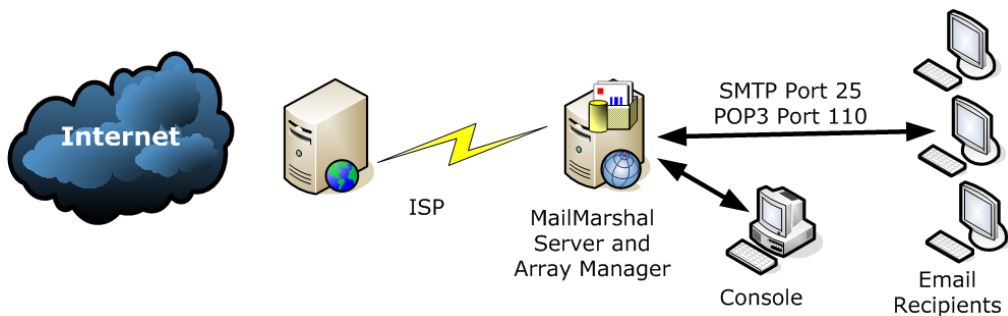
You can configure a standalone installation of MailMarshal SMTP in the following ways:

- As a POP3/SMTP server
- As an internal email relay to your email server
- On your existing email server

Each option provides all the required functions of an email gateway. Other variations are also possible.

### ***MailMarshal SMTP as Email Server***

You can install MailMarshal SMTP to function as a POP3/SMTP email server, providing all email server functions for a small organization, as shown in the following figure.

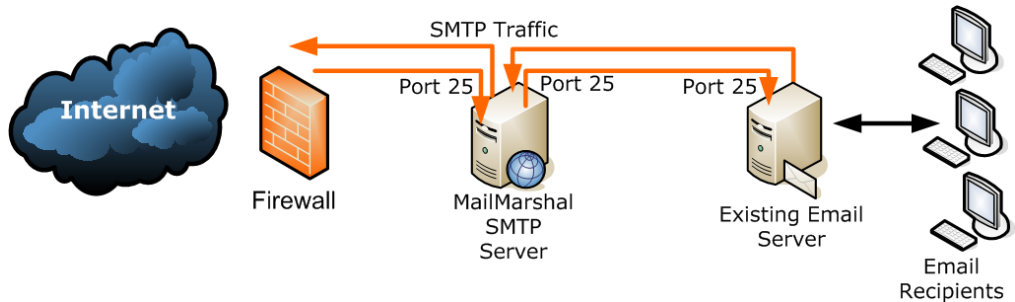


In this scenario, MailMarshal SMTP receives and processes all incoming email. MailMarshal SMTP receives email on port 25 from within the organization and delivers email to internal POP3 mailboxes on port 110. MailMarshal SMTP receives and sends email to and from external addresses over your Internet link.

For this configuration, install the Server and Array Manager components on a single computer. Most organizations that choose this configuration can also install Microsoft SQL Server or SQL Express on the same computer to host the MailMarshal SMTP database.

## ***MailMarshal SMTP as an Internal Email Relay***

You can install MailMarshal SMTP on a separate computer to act as an email relay within an organization, as shown in the following figure.



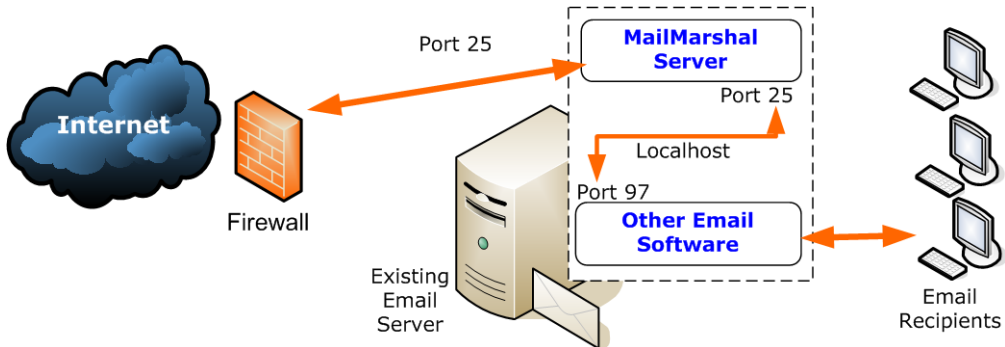
This option is suitable for small to medium-sized organizations with a single Internet gateway and email server. In this scenario, the MailMarshal SMTP Server receives inbound email on port 25, processes it, and forwards it for delivery to the existing email server. The email server forwards all outbound messages to the MailMarshal SMTP Server for processing and delivery.

For this configuration, install the MailMarshal SMTP Server and Array Manager components on a separate computer from the existing email server. Set the Domain Name Service Mail Exchange (DNS MX) records or firewall relay settings so the MailMarshal SMTP Server receives all inbound email.

Most organizations that choose this configuration can also install Microsoft SQL Server or SQL Express on the same computer to host the MailMarshal SMTP database.

## ***MailMarshal SMTP on Existing Email Server***

You can install MailMarshal SMTP on your existing email server computer, as shown in the following figure. The existing server could be a Microsoft Small Business Server (SBS).



MailMarshal SMTP receives all inbound email on default SMTP port 25, processes the email, and forwards email to the existing email server using the local host IP address on port 97 for delivery. The existing email server forwards outbound email to MailMarshal SMTP on port 25 using the local host IP address.

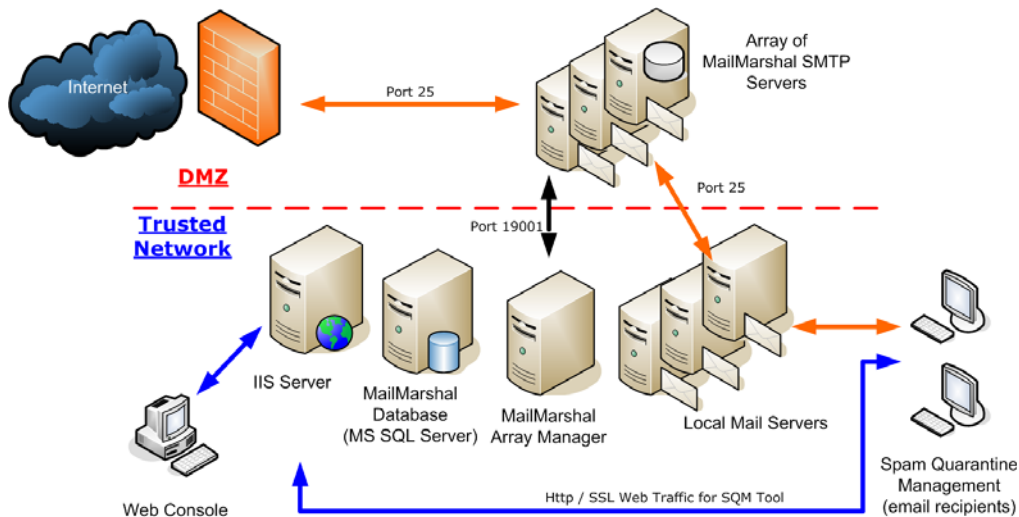
In this case, your email server must have sufficient resources to support both MailMarshal SMTP and another email server application. Install the MailMarshal SMTP Server and Array Manager components on your existing email server. Many organizations that choose this configuration can also install Microsoft SQL Server or SQL Express on the same computer to host the MailMarshal SMTP database.

When you install MailMarshal SMTP on the same physical server as the existing email server software, normally you do not need to change the inbound routing. However, because MailMarshal SMTP takes on the role of listening for SMTP traffic on port 25, you must configure your existing email server to listen for SMTP traffic on another port. Many organizations commonly use port 97 for this purpose, but you can configure your existing email server to listen on any free TCP port.

This configuration is not suitable if you have multiple internal email servers (SMTP or Exchange). With multiple internal email servers, install MailMarshal SMTP on a separate computer as an email relay. For more information, see “MailMarshal SMTP as an Internal Email Relay” on page 21.

## Array Installation

You can install an array of MailMarshal SMTP Servers in a variety of configurations to manage email for larger enterprises. MailMarshal SMTP provides a broad range of enterprise configurations that can include redundancy and failover support. The following figure shows a typical MailMarshal SMTP array configuration.



In this scenario, you can install the MailMarshal SMTP Server component on a number of computers to create an array of MailMarshal SMTP email processing servers in a Demilitarized Zone (DMZ). The DMZ is a part of a local network that has controlled access both to the Internet and to the internal network of the organization.

To provide load balancing, you can install the email processing servers in a cluster using third-party software, such as a Datacenter Server.

A distributed enterprise with more than one email gateway can install one or more MailMarshal SMTP Servers at each gateway. If you use the same email policy at all locations, you can control the MailMarshal SMTP configuration and perform logging for all gateways using a single MailMarshal SMTP Array Manager. All MailMarshal SMTP Servers must be able to communicate with the Array Manager computer over port 19001.

The MailMarshal SMTP Servers receive all incoming email on port 25. MailMarshal SMTP Servers transfer email to and from local email servers on port 25. The MailMarshal SMTP Array Manager requires a single port opening to the DMZ to configure the MailMarshal SMTP Servers and receive log data (port 19001 by default).

Install the MailMarshal Array Manager, and the database if possible, on a dedicated computer inside the trusted network. The location of the Array Manager can affect the performance of the administration and configuration tools used in MailMarshal, but does not affect email processing performance.

For best results, install the MailMarshal SMTP Array Manager component in one of the following locations, listed from most-preferred to least-preferred:

- On the same server as the Microsoft SQL Server hosting the database. Since the Array Manager is the only MailMarshal SMTP component that communicates directly with the database, installing the Array Manager on the computer that hosts Microsoft SQL Server or SQL Express results in the most efficient operation.
- On another computer in the network close to the computer hosting the database over a high-speed network connection.
- On an Active Directory Global Catalog or other Directory Server. The Array Manager communicates regularly to the Global Catalog if you are running Active directory, or through LDAP to another existing Directory Server.

You can install the MailMarshal Configurator, Console, or Reports user interfaces on one or more computers in the local network.

To use the MailMarshal SMTP Web Console or enable your users to manage quarantined email with the Spam Quarantine Management Website, install the MailMarshal SMTP Web Components on a Microsoft IIS server domain member inside the network.

## HARDWARE AND SOFTWARE REQUIREMENTS

Depending on the installation scenario you select and your estimated email volume, the specification for computers on which you install MailMarshal SMTP components can vary. The following sections specify the recommended hardware and software for various computers where you may be installing MailMarshal SMTP components. Consider all the requirements before mapping your MailMarshal SMTP installation.

*Tip: Additional information is available in the MailMarshal SMTP Sizing Guide.*

The MailMarshal SMTP product CD includes many prerequisite software updates, including SQL Express, required service packs, MDAC, and ASP.NET Framework. If you install MailMarshal SMTP from a Web download, you may have to download software you need from the vendor sites. To avoid a system restart during product installation, install any prerequisite software on your computers before you start installing MailMarshal SMTP.

For more information about the latest requirements and supported environments, see the M86 Security Knowledge Base.

### Standalone Installation Requirements

In standalone installations, computer requirements for the MailMarshal SMTP components may vary depending on whether you use MailMarshal SMTP as the POP3 email server or relay, or if you plan to install MailMarshal SMTP on an existing email server.



The following table lists system requirements for installing the MailMarshal SMTP Server, Array Manager, and selected database on a single computer.

MailMarshal SMTP supports use of SQL Express or Microsoft SQL Server as host database.



**Note:** *SQL Server 2008 or SQL Express 2008 has additional prerequisites, including .NET 3.5 SP1 and Windows Installer 4.5*

If you install MailMarshal SMTP on an existing email server, the minimum hardware requirements may be greater than those shown in the table, depending on the number of users and typical email volume.

Category	Requirements
Processor	<b>Minimum:</b> Pentium 4
Disk Space	<b>Minimum:</b> 10GB (NTFS)
Memory	<b>Minimum:</b> 2GB (1 GB if the database is hosted on another server)
Supported Operating System	<ul style="list-style-type: none"> <li>• <i>Windows Server 2008 including R2</i></li> <li>• <i>Windows 7</i></li> <li>• <i>Windows Vista with Service Pack 1</i></li> <li>• <i>Windows Server Standard or Enterprise 2003 with Service Pack 2</i></li> <li>• <i>Windows XP Professional with Service Pack 3 <b>as a domain member</b></i></li> </ul>
Network Access	<ul style="list-style-type: none"> <li>• <i>TCP/IP protocol</i></li> <li>• <i>Domain structure</i></li> <li>• <i>External DNS name resolution - DNS MX record to allow MailMarshal SMTP Server to receive inbound email</i></li> </ul>

Category	Requirements
Software	<ul style="list-style-type: none"> <li>• <i>Database server: SQL Server 2008 or SQL 2008 Express (SP1), SQL Server 2005 or SQL 2005 Express (SP2)</i></li> <li>• <i>Antivirus scanning software supported by MailMarshal SMTP. For more information, see “Supported Antivirus Software” on page 38.</i></li> </ul>
Port Access	<ul style="list-style-type: none"> <li>• <i>Port 25 - Inbound SMTP and to email servers</i></li> <li>• <i>Port 53 - for DNS external email server name resolution (TCP and UDP)</i></li> <li>• <i>Port 80 (HTTP) and Port 443 (HTTPS) - for SpamCensor, SpamProfiler, and Blended Threats Module updates (Proxy usage is supported)</i></li> <li>• <i>Port 1433 - for connection to SQL Server database and Reports Console computers</i></li> <li>• <i>If installed on an existing email server: Port 97 or another available port - for email transfer between MailMarshal SMTP and the other software</i></li> <li>• <i>If serving as a POP3 email server: Port 110 - for email transfer to POP3 mailboxes</i></li> </ul>

When processing large volumes of email, disk I/O can become a limitation. To provide optimal throughput in this case, plan to include dual drives so you can install the MailMarshal SMTP Server components on one drive and the database and Unpacking folder on a separate physical drive. For more information about choosing folder locations, see “Understanding MailMarshal SMTP Folder Locations” on page 37.

To provide redundancy, plan for quad drives configured as two mirrored pairs. For more information to determine your configuration needs, see the White Paper titled “MailMarshal SMTP Sizing Guide” at [www.m86security.com](http://www.m86security.com).

## Array Installation Requirements

In an array installation scenario, you may plan for several MailMarshal SMTP Servers and one Array Manager computer. The following sections provide hardware and software requirements for MailMarshal SMTP Server and Array Manager computers.

For more information to determine your specific requirements, see the “MailMarshal SMTP Sizing Guide” White Paper, at [www.m86security.com](http://www.m86security.com).

### *Server Requirements*

The following table lists system requirements for a MailMarshal SMTP Server computer in an array configuration.

Category	Requirements
Processor	<b>Minimum:</b> Pentium 4
Disk Space	<b>Minimum:</b> 10GB (NTFS)
Memory	<b>Minimum:</b> 1GB
Supported Operating System	<ul style="list-style-type: none"> <li>• <i>Windows Server 2008 including R2</i></li> <li>• <i>Windows 7</i></li> <li>• <i>Windows Vista with Service Pack 1</i></li> <li>• <i>Windows Server Standard or Enterprise 2003 with Service Pack 2</i></li> <li>• <i>Windows XP Professional with Service Pack 3 as a <b>domain member</b></i></li> </ul>
Network Access	<ul style="list-style-type: none"> <li>• <i>TCP/IP protocol</i></li> <li>• <i>Domain structure</i></li> <li>• <i>DNS service available</i></li> </ul>
Software	Antivirus scanning software supported by MailMarshal SMTP. For more information, see “Supported Antivirus Software” on page 38.

Category	Requirements
Port Access	<ul style="list-style-type: none"> <li>• <i>Port 25 - Inbound SMTP and email forwarding to email servers in trusted network</i></li> <li>• <i>Port 53 - DNS external email server name resolution (TCP and UDP)</i></li> <li>• <i>Port 80 (HTTP) and Port 443 (HTTPS) - for SpamProfiler and Blended Threats Module updates (Proxy usage is supported)</i></li> <li>• <i>Port 19001 - Communication with MailMarshal SMTP Array Manager in trusted network</i></li> </ul>

When processing large volumes of email, disk I/O can become a limitation. To provide optimal throughput in this case, you may want to plan for dual drives in the MailMarshal SMTP Server computer so you can install Server components on one drive and the Unpacking folder on a separate physical drive. For more information about choosing folder locations, see “Understanding MailMarshal SMTP Folder Locations” on page 37.

To provide redundancy, you may want to plan for quad drives configured as two mirrored pairs. For more information about determining your configuration needs, see the “MailMarshal SMTP Sizing Guide” White Paper, at [www.m86security.com](http://www.m86security.com)

## ***Array Manager Requirements***

The following table lists system requirements for a MailMarshal SMTP Array Manager computer also hosting the SQL Express or Microsoft SQL Server database.

Category	Requirements
Processor	<b>Minimum:</b> Pentium III 1.0 GHz
Disk Space	<b>Minimum:</b> 10GB (NTFS)

Category	Requirements
Memory	<b>Minimum: 2GB</b>
Supported Operating System	<ul style="list-style-type: none"> <li>• <i>Windows Server 2008 including R2</i></li> <li>• <i>Windows 7</i></li> <li>• <i>Windows Vista with Service Pack 1</i></li> <li>• <i>Windows Server Standard or Enterprise 2003 with Service Pack 2</i></li> <li>• <i>Windows XP Professional with Service Pack 3 as a <b>domain member</b></i></li> </ul>
Network Access	<ul style="list-style-type: none"> <li>• <i>TCP/IP protocol</i></li> <li>• <i>Domain structure</i></li> <li>• <i>DNS service available</i></li> </ul>
Software	<ul style="list-style-type: none"> <li>• <i>Database server: SQL Server 2008 or SQL 2008 Express (SP1), SQL Server 2005 or SQL 2005 Express (SP2). For more information about database considerations, see “Database Software Considerations” on page 35. SQL Server 2008 versions have additional prerequisites, including .NET 3.5 SP1 and Windows Installer 4.5</i></li> <li>• <i>MDAC 2.7 or if using named database instances, MDAC 2.8</i></li> <li>• <i>Antivirus scanning software supported by MailMarshal SMTP. For more information, see “Supported Antivirus Software” on page 38.</i></li> </ul>
Port Access	<ul style="list-style-type: none"> <li>• <i>Port 80 (HTTP) and Port 443 (HTTPS) - SpamCensor updates (Proxy usage is supported)</i></li> <li>• <i>Port 1433 - Connection from Reports Console computers</i></li> <li>• <i>Port 19001 - Communication with MailMarshal SMTP Servers in DMZ</i></li> </ul>

If you install the Array Manager component on a computer running Windows Server or Enterprise 2003, connecting Console computers should reside in the same domain or in a trusted domain.

## Web Components Requirements

To use the MailMarshal SMTP Spam Quarantine Management Website or Web Console, install the MailMarshal SMTP Web Components on a computer running Microsoft Internet Information Services (Microsoft IIS). The following table lists system requirements and recommendations for the computer running Microsoft IIS.

Category	Requirements
Processor	<b>Minimum:</b> Pentium III 1.0 GHz <b>Recommended:</b> Pentium III 2.0 GHz
Disk Space	<b>Minimum:</b> 100MB <b>Recommended:</b> 500MB
Memory	<b>Minimum:</b> 512MB <b>Recommended:</b> 1024MB
Supported Operating System	<ul style="list-style-type: none"> <li>• <i>Windows Server 2008 including R2</i></li> <li>• <i>Windows Server, Enterprise, or Web Edition 2003 with Service Pack 2</i></li> <li>• <i>Windows 7</i></li> <li>• <i>Windows Vista with Service Pack 1</i></li> <li>• <i>Windows XP Professional with Service Pack 3 (may limit number of users accessing Web services)</i></li> </ul>
Network Access	<ul style="list-style-type: none"> <li>• <i>TCP/IP protocol</i></li> <li>• <i>Domain structure</i></li> <li>• <i>DNS service available</i></li> </ul>
Software	Microsoft Internet Information Services 5.1 or above Microsoft ASP.NET Framework 3.5 SP1

Use a secure (HTTPS) website to protect user data and authentication information. The Web components support browsing from Internet Explorer 6 or later clients.

There are additional requirements to install Web components on a computer running a Windows Domain Controller. For more information, see the M86 Security Knowledge Base.

## Configurator or Console User Interface Requirements

The following table lists system requirements and recommendations for computers on which you want to install the MailMarshal SMTP Configurator or Console user interfaces.

Category	Requirements
Processor	<b>Minimum:</b> Pentium III 500 MHz <b>Recommended:</b> Pentium III 1.0 GHz
Disk Space	<b>Minimum:</b> 100MB <b>Recommended:</b> 500MB
Memory	<b>Minimum:</b> 256MB <b>Recommended:</b> 512MB
Supported Operating System	<ul style="list-style-type: none"> <li>• <i>Windows XP Professional with Service Pack 3</i></li> <li>• <i>Windows Vista with Service Pack 1</i></li> <li>• <i>Windows 7</i></li> <li>• <i>Windows Server 2003 with Service Pack 2 (all editions except Web)</i></li> <li>• <i>Windows Server 2008 including R2</i></li> </ul>
Network Access	<ul style="list-style-type: none"> <li>• <i>TCP/IP protocol</i></li> <li>• <i>Domain structure</i></li> <li>• <i>DNS service available</i></li> <li>• <i>If running Web Console, access to Microsoft IIS server</i></li> </ul>

Category	Requirements
Software	MMC 1.2 or later Internet Explorer 5.5 or later
Port Access	NetBIOS - Communication with Array Manager computer

## Reports User Interface Requirements

The following table lists system requirements and recommendations for computers on which you want to install the MailMarshal SMTP Reports user interface.

Category	Requirements
Processor	<b>Minimum:</b> Pentium III 500 MHz <b>Recommended:</b> Pentium III 1.0 GHz
Disk Space	<b>Minimum:</b> 100MB <b>Recommended:</b> 500MB
Memory	<b>Minimum:</b> 256MB <b>Recommended:</b> 512MB
Supported Operating System	<ul style="list-style-type: none"> <li>• <i>Windows XP Professional with Service Pack 3</i></li> <li>• <i>Windows Vista with Service Pack 1</i></li> <li>• <i>Windows 7</i></li> <li>• <i>Windows Server 2003 with Service Pack 2 (all editions except Web)</i></li> <li>• <i>Windows Server 2008 including R2</i></li> </ul>
Network Access	Install on or provide access to computer hosting MailMarshal SMTP database
Software	MDAC 2.7 <i>or if using named database instances</i> , MDAC 2.8
Port Access	Port 1433 - Access to the Microsoft SQL Server or SQL Express database computer



# DATABASE SOFTWARE CONSIDERATIONS

MailMarshal SMTP supports use of SQL Express or Microsoft SQL Server. To estimate the size of your MailMarshal SMTP database and determine whether to use SQL Express or Microsoft SQL Server, review the following sample worksheet and complete My Worksheet with appropriate estimates.

<b>Sample Worksheet</b>		
Number of users	=	100
Average number of valid and quarantined email messages per user per day	x	70
Number of days in log data retention period	x	100
Safety margin	x	1.25
Total database size in bytes for retention period	=	875,000 bytes
Total database size in MB for retention period (divide by 1024)	=	855 MB

The following blank worksheet lets you estimate the database size requirement based on your enterprise use.

<b>My Worksheet</b>		
Number of users	=	
Average number of valid and quarantined email messages per user per day	x	
Number of days in log data retention period	x	
Safety margin	x	
Total database size in bytes for retention period	=	
Total database size in MB for retention period (divide by 1024)	=	

The following table shows calculations with example data you can use as a guideline if the assumptions for email volume, log retention duration, and safety margin are appropriate for you.

Users	Email / Day / User	Days to Keep Logs	Safety Margin	Bytes	MB	GB	DB to Use
100	70	100	1.25	875,000	854	0.83	Express
200	70	100	1.25	1,750,000	1709	1.67	Express
225	70	100	1.25	1,968,750	1923	1.88	Express
250	70	100	1.25	2,187,500	2136	2.09	SQL
500	70	100	1.25	4,375,000	4272	4.17	SQL
1000	70	100	1.25	8,750,000	8545	8.34	SQL
2000	70	100	1.25	17,500,000	17090	16.69	SQL
5000	70	100	1.25	43,750,000	42725	41.72	SQL

For small installations, when the MailMarshal SMTP email processing server is on a computer other than the Array Manager and database server, the database server will have a light load on the database. However, using the Consoles and Reports user interfaces places additional load on the database.

If you have more than 500 email users, the Microsoft SQL Server memory footprint can become quite high. In this case, you can add memory to the Microsoft SQL Server computer (3GB or more) so Microsoft SQL Server can use its maximum of 2GB and still reserve memory for the Array Manager, operating system, and other system demand. Other environment factors may also affect performance and throughput rates.

# UNDERSTANDING MAILMARSHAL SMTP FOLDER LOCATIONS

By default, the installation process creates several folders in the MailMarshal SMTP program installation folder. For many cases, the default folder locations work well.

In some cases, you can enhance product performance by creating these folders on another local physical hard drive. You can choose different locations on each email processing server. The folders are defined as follows:

## Logging

MailMarshal SMTP uses this folder to store text logs that provide details of each action taken by each MailMarshal SMTP service. By default, MailMarshal SMTP retains logs for five days. The files can be large when email volume is high.



**Note:** *Compressing this folder with Windows file system compression reduces the disk space required and does not affect performance in most cases. Do not use compression for any other MailMarshal SMTP folders.*

## Queues

MailMarshal SMTP uses this folder and subfolders to hold messages for processing or sending. In most cases, these folders do not grow large. However, if MailMarshal SMTP cannot connect to upstream or downstream servers, the data in the folders can grow quickly.

## Unpacking

MailMarshal SMTP uses this folder to unpack messages and extract their content, including attachments such as archive files. The size of this folder is relatively small. Because the Server creates and deletes files repeatedly, this area of the disk can become fragmented, which can have an adverse affect on other applications running on the server. You can improve performance by placing this folder on a separate physical disk drive from other MailMarshal SMTP components.

## Quarantine

MailMarshal SMTP uses this folder as the default location for all quarantine folders. MailMarshal SMTP stores all quarantined messages in subfolders of this folder, including any archived messages and messages in the Mail Recycle Bin. Ensure the disk drive where this folder resides has enough free space to accommodate the messages. The space required varies depending on your retention policies for quarantined messages. You can move individual folders to physically separate places on the server (not available for appliances). For more information, see “Working with Folders” on page 215.



**Note:** MailMarshal SMTP does not accept new messages if there is less than 512MB of free disk space available for the Queues, Unpacking, Quarantine, or Logging folders. MailMarshal SMTP slows down mail acceptance if there is less than 1GB of free space available for these folders. This is a significant increase in required space from earlier versions.

Appliance nodes do not accept messages if there is less than 2GB of free space available for these folders. Appliance nodes slow down mail acceptance if there is less than 5GB of free space available for these folders.

For more information, see M86 Security Knowledge Base article Q11669.

# SUPPORTED ANTIVIRUS SOFTWARE

MailMarshal SMTP supports a number of third-party antivirus scanners to scan for (and in some cases clean) virus-laden email. The scanners offering a MailMarshal SMTP specific DLL file offer much higher throughput and enhanced features. command line scanners are suitable for basic scanning in relatively small organizations.



**Note:** Appliance installations are pre-configured using McAfee for Marshal. Appliance installations cannot currently use other scanners.

M86 Security licenses the Marshal antivirus solutions separately from the MailMarshal SMTP product. Trial versions of the Marshal antivirus solutions are available from the installation CD-ROM or as downloads from [www.m86security.com](http://www.m86security.com).

MailMarshal SMTP actively supports the antivirus software brands listed in the following table. For more information about currently supported versions, see M86 Security Knowledge Base article Q10923.

Antivirus Application	Features
Computer Associates AntiVirus (formerly eTrust EZAntiVirus or InoculateIT)	Command line scanner
McAfee Command Line	Command line scanner
McAfee for Marshal	DLL, cleaning
Marshal Norman Virus Control	DLL, cleaning, Sandbox II
NOD32 Command Line	Command line scanner
Sophos Anti-Virus	DLL, cleaning
Sophos for Marshal	DLL, cleaning
Symantec AntiVirus Scan Engine	DLL, cleaning, remote installation

## COLLECTING INFORMATION FOR INSTALLATION

Before you install MailMarshal SMTP, you may want to collect the following information about your environment. When you run the Configuration Wizard after you install the product, having the following details handy can help you quickly configure MailMarshal SMTP.

Information required	My information
Names of computers where you plan to install MailMarshal SMTP components including: Servers, Array Manager, database, Configurator, and Console, and optionally, Reports and Web components.	

Information required	My information
Prerequisite software for each computer where you will install software and the best time to restart each system, if necessary.	
DNS server administrator of domains for which MailMarshal SMTP will process email and best time to make and propagate DNS changes.	
Firewall administrator contact information, and best time to make and propagate firewall settings changes.	
Antivirus software to use with MailMarshal SMTP.	
Company name for MailMarshal SMTP license.	
Names of local domains for which MailMarshal SMTP will process email (for example, <i>mycompany.com</i> or <i>pop.mycompany.com</i> )	
IP address and access port for your existing Microsoft SQL server computer.	
IP address and access port for your existing local email server.	
If using POP3 mailboxes, decide how to route email for undefined accounts.	
IP address and logon credentials for your directory server (Active Directory or LDAP).	
Email address where MailMarshal SMTP will send administrator notification emails (existing or new account).	
Email address email notifications to recipients will be from (reply to address) (existing or new account).	

---

<b>Information required</b>	<b>My information</b>
IP addresses of primary and optional secondary DNS servers MailMarshal SMTP will use for internal and external domain name resolution.	
Server name, fully qualified domain name, or IP address of host and optional alternate to forward external email.	
Existing outbound delivery details and required routing changes.	
Existing inbound delivery details and required routing changes.	





---

## Chapter 3

# Installing and Configuring MailMarshal SMTP

Before you install MailMarshal SMTP, be sure to complete the steps in the planning checklist. For more information, see “Planning Checklist” on page 13.

When you complete the planning checklist, you should know if you are planning a standalone or array installation, which MailMarshal SMTP components you want to install, and on which computers you plan to install each component. Collect the information listed in “Collecting Information for Installation” on page 39 before you run the Configuration Wizard.

If you are upgrading a MailMarshal SMTP installation from an earlier version, there are a number of other considerations. For more information, see “Upgrading MailMarshal SMTP” on page 76.

## INSTALLATION CHECKLIST

To install MailMarshal SMTP, complete each step in the checklist. For more information, refer to the appropriate section.

<input checked="" type="checkbox"/>	Steps	See Section
<input type="checkbox"/>	1. Install prerequisite software.	“Installing Prerequisite Software” on page 45
<input type="checkbox"/>	2. <i>If you are installing MailMarshal SMTP on a standalone server, install all components.</i>	“Installing MailMarshal SMTP on a Standalone Server” on page 46

<input checked="" type="checkbox"/>	<b>Steps</b>	<b>See Section</b>
<input type="checkbox"/>	<b>3.</b> <i>If you are installing MailMarshal SMTP on an array of servers, install required components on each computer.</i>	"Installing MailMarshal SMTP as an Array" on page 48
<input type="checkbox"/>	<b>4.</b> Run the Configuration Wizard.	"Running the Configuration Wizard" on page 56
<input type="checkbox"/>	<b>5.</b> Configure email routing as necessary to direct incoming mail to MailMarshal SMTP and mail delivery as needed.	"Configuring Email Routing" on page 61
<input type="checkbox"/>	<b>6.</b> Create connections to your directory services to populate MailMarshal SMTP groups.	"Creating Directory Connectors" on page 62
<input type="checkbox"/>	<b>7.</b> Configure MailMarshal SMTP to use your antivirus product. ( <i>Not required for Appliance installations.</i> )	"Configuring Antivirus Scanning" on page 65
<input type="checkbox"/>	<b>8.</b> Optionally, install MailMarshal SMTP Reports.	"Installing MailMarshal SMTP Reports" on page 69
<input type="checkbox"/>	<b>9.</b> Optionally, install MailMarshal SMTP Web components.	"Installing and Customizing Web Components" on page 70
<input type="checkbox"/>	<b>10.</b> Optionally, install additional Configurator or Console user interfaces on additional computers.	"Installing Additional User Interfaces" on page 75

# INSTALLING PREREQUISITE SOFTWARE

Before installing MailMarshal SMTP, install any prerequisite software the MailMarshal SMTP components require. This will simplify troubleshooting, and allow you to avoid restarting your computer during the product installation process. For more information about required software for each MailMarshal SMTP computer in your configuration, see “Hardware and Software Requirements” on page 26.

The MailMarshal installation CD-ROM includes most prerequisite software MailMarshal SMTP requires. If you download the installation package from the M86 Security website, the package includes many prerequisites, and provides links that allow you to download the remaining prerequisites from M86 Security or vendor sites.

If you plan to configure MailMarshal SMTP to use an antivirus solution, install your antivirus product on MailMarshal SMTP Server computers before installing MailMarshal SMTP. The MailMarshal SMTP setup program Antivirus tab provides links to some supported antivirus products. For information about supported antivirus products, see “Supported Antivirus Software” on page 38, and the M86 Security Knowledge Base. You can also configure MailMarshal SMTP to use a centrally installed antivirus product. For more information, see “Configuring Antivirus Scanning” on page 65.



**Note:** *Appliance installations are pre-configured with the McAfee for Marshal solution. Antivirus configuration is not required for these installations.*

## **To install prerequisite software or included antivirus products:**

1. Run the setup program from the MailMarshal SMTP installation.
2. On the Prerequisites or Antivirus tab, click the link for the product you want to install or download.
3. Follow the instructions until the product is installed.

4. Ensure that no Simple Mail Transport Protocol (SMTP) services are running on the computer, and disable any SMTP filtering or blocking components.
5. When product installation is complete, return to the setup program.

## INSTALLING MAILMARSHAL SMTP ON A STANDALONE SERVER

You can install the MailMarshal Server, Array Manager, and database on one computer. For more information about standalone MailMarshal SMTP installation, see “Standalone Installation” on page 19 and “Standalone Installation Requirements” on page 26

Use the **Basic Install** option to install MailMarshal SMTP on a standalone computer. The basic install option installs MailMarshal SMTP using the default installation and folder locations. If you are installing from the CD-ROM or web “with SQL Express” version, the Basic Install installs a local instance of SQL Express 2008 if necessary. To use a different SQL Server computer, select **Custom Install**. See the instructions under “Installing a MailMarshal SMTP Array Manager” on page 49.



**Note:** The **Basic Install** uses a default set of install options required to use SQL Express with MailMarshal SMTP. These include Mixed Mode authentication and TCP connections. If you want to review and alter other installation options (such as instance name and install location), M86 Security recommends you install SQL Express 2008 before installing MailMarshal SMTP. See the Prerequisites tab of the MailMarshal SMTP setup program.

If you later want to specify alternate folder or database locations for MailMarshal SMTP, use the MailMarshal SMTP Server Tool. For more information, see “Changing Folder Locations” on page 297.

### To install MailMarshal SMTP on a standalone computer using the default MailMarshal SMTP folder locations:

1. Ensure you have installed all prerequisite software specified for a standalone installation. For more information, see “Standalone Installation Requirements” on page 26 and “Installing Prerequisite Software” on page 45.
2. Log on to the computer as a member of the local Administrators group.
3. Close any open applications.
4. Run the setup program from the MailMarshal SMTP installation CD or download.
5. On the Setup tab, click **Install MailMarshal SMTP**.
6. On the Welcome window, click **Next**.
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement**, and then click **Next**.
9. On the Setup Type window, select **Basic Install**, and then click **Next**.



**Note:** The **Basic Install** option enables the default set of MailMarshal SMTP spam blocking rules. If you want to compare MailMarshal SMTP to another anti-spam product, you can choose **Monitoring Install**. This option enables the Monitor Only rules but does not block any spam. By running MailMarshal SMTP with the Monitor Only rules enabled concurrently with another product for a period of time, you can compare the spam detection rates of the products.

#### 10. If you choose to install SQL Express:

- a. Note that SQL Express requires .NET 3.5 SP1, and Windows Installer 4.5. The setup program prompts you to enter a strong password for the SQL Express sa account.
- b. SQL Express setup executes in silent mode. This process may take a number of minutes. Once installation is complete, MailMarshal SMTP installation continues.

11. The Basic Install process attempts to connect to a SQL instance on the local computer using Windows authentication, and create a database named Mail Marshal . I



**Note:** If the process encounters problems connecting, you can use **Custom Install** for more options. See the instructions under “Installing a MailMarshal SMTP Array Manager” on page 49. If the database already exists, you can choose to use or re-create it. If you are unsure, use **Custom Install** to create a database with a different name.

12. The Settings Summary window displays the folder locations and database details for the installation. Review the settings, and then click **Next**.
13. On the Ready to Install window, click **Install**. The setup program displays a progress bar until the program is installed.
14. On the Finished window, ensure **Run Configuration Wizard** is selected, and then click **Finish**.

You must run the Configuration Wizard before MailMarshal SMTP can receive email and apply rules. For more information, see “Running the Configuration Wizard” on page 56.

## INSTALLING MAILMARSHAL SMTP AS AN ARRAY

A MailMarshal SMTP array consists of a MailMarshal **Array Manager** and one or more MailMarshal **Servers**. The Array Manager hosts the user interfaces and manages the database connection. The Array Manager exports the same rules and other configuration to all MailMarshal Servers connected to it.

First, install the Array Manager and database on a computer in the trusted network. Then, install the MailMarshal Server software on one or more computers in the DMZ to work as an array of email processing servers. Each MailMarshal Server receives email and processes it using your rules.

Base the number of servers you install on your email volume. You can add servers later as needed. For more information about an array installation and requirements, see “Array Installation” on page 24 and “Array Installation Requirements” on page 29.

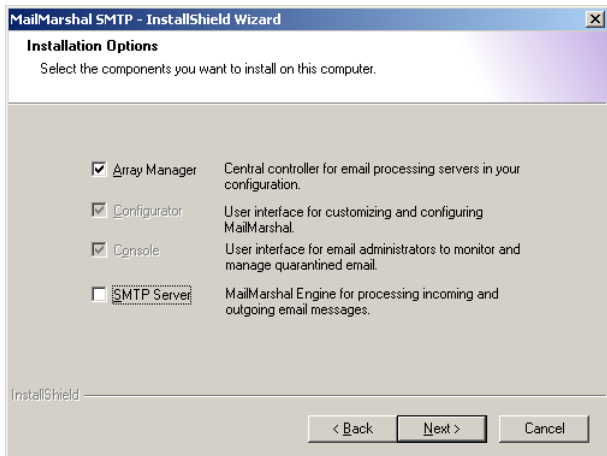
## Installing a MailMarshal SMTP Array Manager

To install MailMarshal SMTP in an array configuration, first install the Array Manager component on the computer you selected as the Array Manager computer.

### To install the Array Manager:

1. Ensure you have installed all prerequisite software specified for an array installation. For more information, see “Array Manager Requirements” on page 30 and “Installing Prerequisite Software” on page 45.
2. Log on to the computer as a member of the local Administrators group.
3. Close any open applications.
4. Run the setup program from the MailMarshal SMTP installation CD-ROM or Web download.
5. On the Setup tab, click **Install MailMarshal SMTP**.
6. On the Welcome window, click **Next**.
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement**, and then click **Next**.
9. On the Setup Type window, select **Custom Install**, and then click **Next**.
10. On the Installation Options window, ensure **Array Manager** is selected. The MailMarshal Configurator and Console user interfaces are installed by default when you install the Array Manager component.

**11. Clear **SMTP Server**, and then click **Next**.**



**12. On the Choose Installation Location window, optionally change the installation and folder locations.**



13. On the Database window, set SQL Server options for the MailMarshal SMTP database.

- a. Specify a local or remote SQL server.
- b. Specify a database name (by default, Mail Marshal).



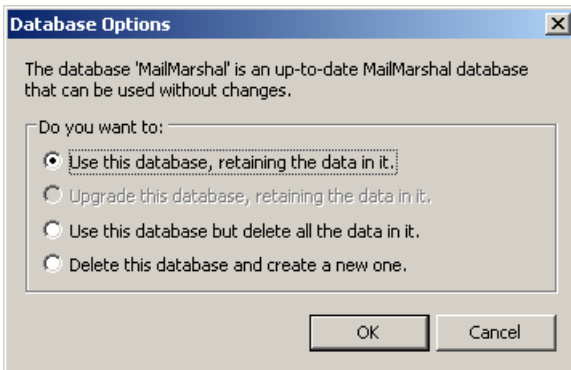
**Tip:** A database name must start with a letter (a..z) or an underscore (\_). The name can also contain digits (0..9). Other characters including the hyphen (-) are generally NOT allowed.

- c. Choose an account to use for database access. This account can be a Windows or SQL Server account. If the SQL Server is on the same computer as MailMarshal SMTP, you can use the system service account (the Local System account used by default to run MailMarshal services). MailMarshal can also configure an “operational user” account with limited permissions, and use this account for most processing. For full information about available database connection and security options, see M86 Security Knowledge Base article Q12939.



**Tip:** You can change the account information later using the MailMarshal SMTP Server Tool.

14. Click **Next**. MailMarshal verifies the database information. If the database you selected already exists, you can choose options to use it, or cancel and provide a different database name. The available options depend on the database that is actually found.



15. Follow the instructions in the setup program until you finish installing MailMarshal SMTP.
16. On the Setup Complete window, ensure **Run Configuration Wizard** is selected, and then click **Finish**.

You must run the Configuration Wizard before MailMarshal SMTP can receive email and apply rules. For more information, see “Running the Configuration Wizard” on page 56.

## Installing a MailMarshal SMTP Server

To complete a MailMarshal SMTP array installation, first install the MailMarshal SMTP Array Manager. Then, follow the steps to install a MailMarshal SMTP Server on additional computers. You can install additional email processing servers initially or add them later as needed.

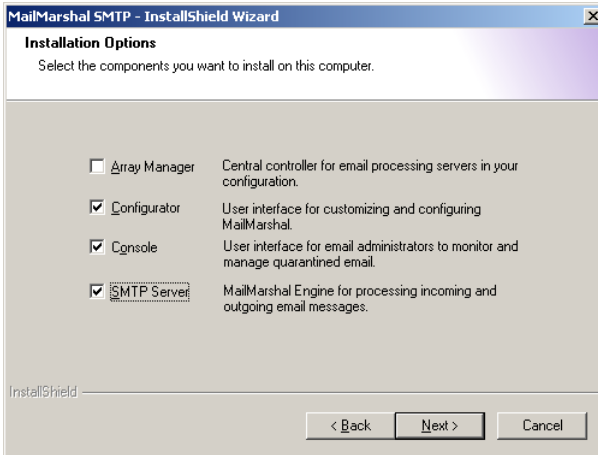


**Note:** If you are creating an Appliance installation, each Server is a hardware appliance. Refer to the Appliance Quick Start Guide for details of appliance setup.

**To install the MailMarshal SMTP Server components:**

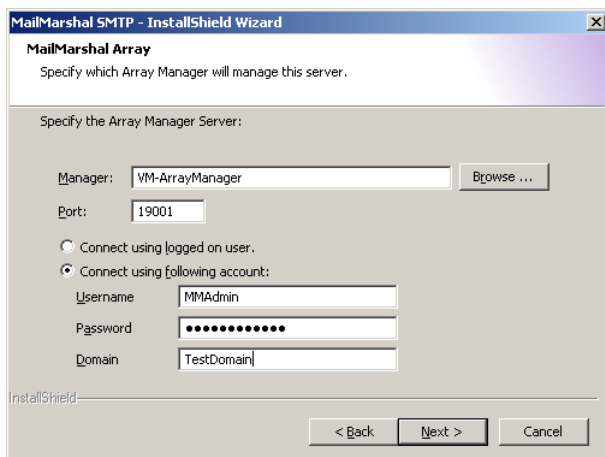
1. Ensure you have installed all prerequisite software specified for a MailMarshal SMTP Server computer. For more information, see “Server Requirements” on page 29 and “Installing Prerequisite Software” on page 45.
2. Log on to the computer you plan to use as a MailMarshal SMTP Server as a member of the local administrator group.
3. Close any open applications.
4. Run the setup program from the MailMarshal SMTP installation kit.
5. On the Setup tab, click **Install MailMarshal SMTP**.
6. On the Welcome window, click **Next**.
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement**, and then click **Next**.
9. On the Setup Type window, select **Custom Install**, and then click **Next**.
10. On the Installation Options window, ensure **SMTP Server** is selected.

## 11. Clear **Array Manager**, and then click **Next**.



12. On the MailMarshal Array window, enter the name of the MailMarshal SMTP Array Manager that you will use to manage policy for this server. The name can be the computer name, IP address, or Fully Qualified Domain Name.
13. *If you have changed the default MailMarshal SMTP port*, enter the new value in the **Port** field.

14. *If you are not logged in as a user with permission to join the MailMarshal SMTP array*, select **Connect using following account** and enter the correct Windows credentials. For more information about setting this permission see “Configuring Manager Security” on page 281.



15. Click **Next**.
16. Continue running the setup program until you finish installing a MailMarshal SMTP Server.
17. On the Setup Complete window, click **Finish** to close the setup wizard. The server retrieves configuration information from the Array Manager immediately and begins accepting email connections.
18. *If you plan to install the MailMarshal SMTP Server on additional computers*, repeat the MailMarshal SMTP Server installation process on the other computers.

# RUNNING THE CONFIGURATION WIZARD

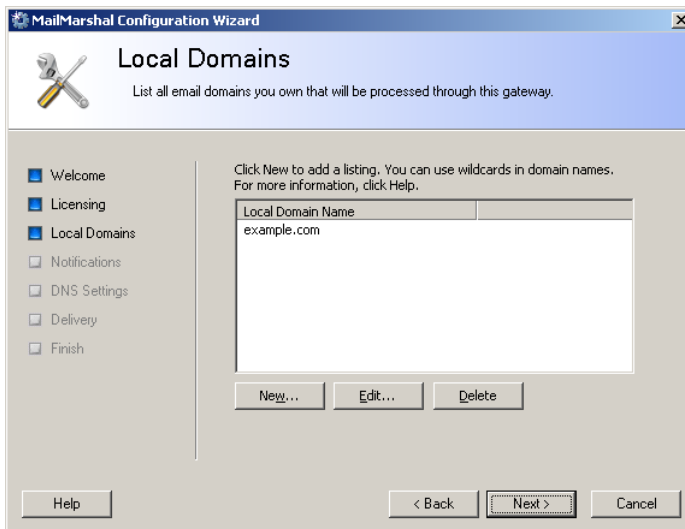
After you have completed a standalone installation or installed the Array Manager component in an array installation, you must run the MailMarshal SMTP Configuration Wizard. This Wizard lets you configure MailMarshal SMTP to accept email and apply rules.

When you click **Finish** on the final window of the MailMarshal SMTP Setup Wizard, by default MailMarshal SMTP runs the Configuration Wizard. If you do not run this wizard after running setup, MailMarshal SMTP runs the wizard the first time you start the MailMarshal SMTP Configurator.


## To run the Configuration Wizard:

1. **If the Configuration Wizard is not running**, start the Wizard by running the MailMarshal SMTP Configurator from the MailMarshal program folder.
2. On the Welcome window, click **Next**.
3. On the Licensing window, type your company or organization name. This information identifies your organization when you request a license key for MailMarshal SMTP. The Licensing window also reports details of your current license. You can enter another license key at a later time. For more information, see “Managing Your MailMarshal SMTP Licenses” on page 257.
4. Click **Next**.
5. On the Local Domains window, enter one or more domain names for which this MailMarshal SMTP server will accept incoming mail.
  - a. Click **New**.
  - b. Enter a domain name and click **OK**.
  - c. Repeat the above steps for each local domain

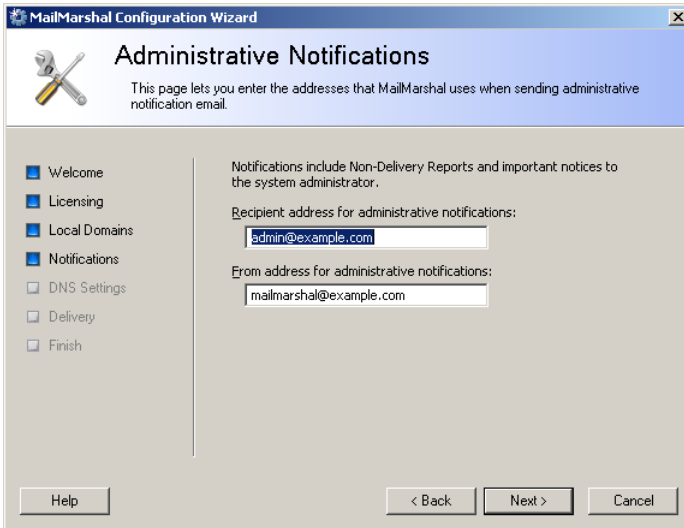
- d. To edit or delete an existing entry, select it and then click the appropriate button.



**6. Click Next.**

 **Note:** You will set the delivery location in a later step. To choose advanced options (such as POP3 delivery and multiple delivery locations), after completing the wizard you can edit Routes in the Configurator.

7. On the Administrative Notifications window, enter email addresses used by automated functions of MailMarshal SMTP:



- a. MailMarshal SMTP sends administrative notifications (such as Dead Letter reports) to the address you specify in the **Recipient Address** field. This address should be a valid and appropriate mailbox or group alias.
- b. MailMarshal SMTP sends administrative and user notifications and other automated email from the address you specify in the **From Address** field. This address should be a valid address to allow for replies to notifications.



8. On the DNS Servers window, enter the addresses of servers MailMarshal SMTP uses for domain name resolution. The wizard pre-populates the fields using Windows DNS settings, but MailMarshal SMTP performs DNS lookups independently of the Windows settings. The DNS servers used by MailMarshal SMTP should be located no further away than your ISP.



**Note:** If MailMarshal SMTP must perform DNS lookups through a firewall, the firewall must permit both TCP and UDP based lookups.

- a. Enter the IP address of the primary DNS server. You must enter a valid server IP address.
- b. Enter a secondary address. You can leave this entry blank, but your configuration is more robust if you supply a secondary DNS server.

The screenshot shows the 'MailMarshal Configuration Wizard' window, specifically the 'DNS Servers' step. The window has a blue header with the title and a close button. Below the header is a sub-header 'DNS Servers' with a wrench and screwdriver icon. The main content area is divided into two sections. On the left is a vertical list of steps: 'Welcome', 'Licensing', 'Local Domains', 'Notifications', 'DNS Settings', 'Delivery', and 'Finish'. 'DNS Settings' is currently selected. On the right, there is instructional text: 'Specify the IP addresses of DNS servers MailMarshal can use to resolve domain names outside your network.' and 'To help you set up this information, the DNS server information below was copied from the network properties of this server. Make changes if required.' Below this text are two input fields: 'Primary DNS Server:' with the value '10 . 67 . 0 . 1' and 'Secondary DNS Server (optional):' with the value '10 . 67 . 0 . 2'. At the bottom of the window are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

- c. Click **Next**.

9. On the Delivery window, specify the methods MailMarshal SMTP will use by default to deliver inbound and outbound email



**Note:** After you complete the wizard, you can configure other delivery options, including POP3 delivery, load balancing, and multiple routes. For more information, see “Configuring Delivery Options” on page 275 and “Customizing Settings for Nodes” on page 286.

- a. Enter the IP address and port of a local server that MailMarshal SMTP will use to deliver all incoming email (addressed to local domains).
- a. Choose to deliver outgoing email directly using DNS lookup, or to forward email to another server for delivery.
- b. **If you select “forward email to another SMTP server”,** specify the server name, fully qualified domain name, or the IP address of the server. For instance, use this option to send all outbound email through the email servers at your ISP.

**MailMarshal Configuration Wizard**

### Delivery

This page allows you to set up the basic delivery methods for incoming (Local Domain) email and outgoing email.

Local Domain email should be forwarded to the following mail server IP/port:

10 . 67 . 1 . 1 | 25

Specify how you want MailMarshal to deliver email to the Internet:

MailMarshal will deliver external email itself using DNS resolution

MailMarshal will forward email to another SMTP server for delivery:

Forwarding Host:

MailMarshal provides a range of rich routing and load balancing capabilities that may be configured after the initial wizard is complete.

Help      < Back      Next >      Cancel

- c. Click **Next**.

**10. Review the Completing window, and then click **Finish**.**

When you complete the Configuration Wizard, MailMarshal SMTP starts the email processing services and opens the Configurator. Use the Configurator to perform additional configuration tasks. You will need to complete some tasks to implement minimum best practices for MailMarshal SMTP installation and email filtering. For more information, see “Configuring Email Routing” on page 61, “Creating Directory Connectors” on page 62, and “Configuring Antivirus Scanning” on page 65.

## CONFIGURING EMAIL ROUTING

After you install MailMarshal SMTP and run the Configuration Wizard, you may need to change the email routing on other computers so the MailMarshal SMTP Server becomes the gateway for incoming and outgoing email. For more information, see “Understanding Installation Scenarios” on page 19. These routing changes can require you to adjust one or more of the following items:

### **DNS MX records**

If you install the MailMarshal SMTP Server on a server with a different name or IP address from your prior email server, change the MX records that control email delivery from the Internet.

### **Internal email server settings**

Configure all other internal email servers within your organization to forward outgoing email to a MailMarshal SMTP Server for delivery. In some cases, you may also want to route email between local domains through MailMarshal SMTP.

### **Port settings**

In some cases, MailMarshal SMTP is configured as a single server on the same physical server as other email software. In this case, change the settings of the other email software to allow MailMarshal SMTP to receive SMTP connections from the Internet on port 25. Configure alternate ports so that MailMarshal SMTP and the other software can exchange email.

### Firewall or relay server settings

If MailMarshal SMTP receives incoming email from a firewall that employs address translation, change the translated address for incoming email to the address of the MailMarshal SMTP Server. If the firewall or another server acts as an email relay, change the address to which it forwards inbound email to the address of the MailMarshal SMTP server.

## CREATING DIRECTORY CONNECTORS

MailMarshal SMTP can apply email policies selectively based on the email address of a local or remote user. Typically, organizations apply policy to groups of local users by retrieving lists of users from an internal directory of email users such as Microsoft Exchange or Lotus Notes. MailMarshal SMTP can also retrieve groups by connecting to a Microsoft Active Directory or an LDAP directory server. Creating MailMarshal SMTP connectors allows you to retrieve your user and group information periodically from these directories.

### To create a directory connector:

1. **If the *MailMarshal SMTP Configurator is not running***, start the MailMarshal SMTP Configurator from the MailMarshal program folder.
2. In the left pane, expand **MailMarshal SMTP Configurator**.
3. Expand **Policy Elements**.
4. Click **Connectors**.
5. On the Action menu, click **New Connector**.



**Note:** For detailed guidance on this wizard, click *Help* on each window.

6. On the Connector Type window, choose the type of directory this connector will access. MailMarshal SMTP supports connections to Microsoft Active Directory and several types of LDAP directories.

- 7. If this is a Microsoft Active Directory connection**, on the Microsoft Active Directory Setting page, choose to connect as anonymous, or as a specific account. If you choose to connect using a specific account, enter the account details, and then click **Next**.
- 8. If this is an LDAP connection**, specify the following information:
- Select a specific type of LDAP directory server from the list, and then click **Next**. MailMarshal SMTP uses appropriate parameters to retrieve group and member details for the type of server you choose.
  - On the LDAP Server and Logon page enter the server name, port, and logon information. For more information, click **Help**. You can connect anonymously or specify an account with required permissions. If you choose to connect using a specific account, specify the account details, and then, click **Next**. If you do not know the required information, contact the administrator of the LDAP server.

The screenshot shows the 'New Connector Wizard' window with the title 'LDAP Server and Logon'. The window contains a sidebar on the left with a tree view showing 'Connector Type' (selected), 'Details', 'LDAP Server' (selected), 'LDAP Search Root', 'Group Attributes', 'User Attributes', 'Reload Schedule', 'General', and 'Finish'. The main area displays the following settings:

- Server name and port:**
  - Server Name: Directory01 (with a 'Browse...' button)
  - Server Port: 389 (with 'Default is 389')
  - Connect using SSL
  - Version: 2 (dropdown menu)
- This server requires me to logon
  - User Name: automation
  - Password: [masked with dots]
  - Domain: [empty]
  - Use Windows Integrated Security (NTLM)

At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

- c. On the LDAP Search Root window identify a search root for this server, and then click **Next**. If you do not know whether a search root is required, contact the administrator of the LDAP server.
- d. *If this is a generic LDAP connection*, on the LDAP Groups and LDAP Users windows, customize the information MailMarshal SMTP will use to query the LDAP server for group names and group members, and then click **Next**. For details of the fields, see Help.



***Note:** The wizard populates default values depending on the server type you selected. You may need to customize the values. Consult the LDAP server documentation and the LDAP server administrator.*

9. On the Reload Schedule window, specify how often MailMarshal SMTP will import directory information through this connector, and then click **Next**.
10. On the Connector Name and Description window, enter a connector name and description, and then click **Next**.
11. On the Finish window, MailMarshal SMTP displays a summary of the settings for the connector. Review the settings, then click **Finish** to create the connector and close the window.

The properties of an LDAP connector include advanced configuration options that allow you to control which email addresses and groups MailMarshal SMTP retrieves. For more information about editing connectors and advanced LDAP configuration, see “Configuring Connectors” on page 177.

# CONFIGURING ANTIVIRUS SCANNING

To work with MailMarshal SMTP, an antivirus product must offer a command-line interface or be supported by a custom MailMarshal SMTP DLL. The scanner must return a documented response indicating whether or not a virus is detected. Most commercially available virus scanners meet these specifications. For more information about supported antivirus products, see M86 Security Knowledge Base article Q10923.

 **Note:** *Appliance installations are pre-configured using McAfee for Marshal. Appliance installations do not need to configure virus scanning.*

To allow MailMarshal SMTP to use your antivirus product to scan email for viruses, first exclude specific MailMarshal SMTP folders from virus scanning. The MailMarshal SMTP Engine service does not run if an antivirus product scans these folders. Then, you must configure MailMarshal SMTP to use the antivirus product you installed.

 **Note:** *The discussion in this section also applies to Anti-spyware scanning products (PestPatrol for Marshal and CounterSpy for Marshal). For more information about the value of anti-spyware scanning, see “Anti-Spyware Scanners” on page 340.*

## Excluding Working Folders From Virus Scanning

MailMarshal SMTP uses a number of folders to process and quarantine email messages, possibly including virus infected messages. MailMarshal SMTP will not operate if these folders are scanned by an antivirus or anti-malware product.

To prevent scanning these working folders, you must configure your scanning products to exclude specific working folders on every MailMarshal Server. You must exclude these working folders even if you do not configure MailMarshal SMTP to scan for viruses using the antivirus product. If the virus scanner does not have the facility to exclude the appropriate folders, you must disable on-access scanning completely for that scanner.

Some scanners also automatically enable an Internet protection feature (for instance, the Marshal Norman Antivirus product). In this case, disable the Internet protection option in addition to disabling the on-access scanning option.

MailMarshal SMTP checks for resident file scanning by writing the `ei car . com` standard test virus file (*not a real virus*) in each of the folders that must be excluded from scanning. If any copy of the test file is removed or cleaned by a resident scanner, or if MailMarshal SMTP is denied access to the files, the MailMarshal SMTP Engine service on the Server does not start and MailMarshal SMTP sends an email notice to the administrator.

If the check succeeds, MailMarshal SMTP deletes copies of the `ei car . com` file, preserving the original in the `Unpacki ng\avcheck` folder.

By default, the MailMarshal SMTP setup program creates working folders in the MailMarshal SMTP installation folder. If you choose a different folder name or drive location when you install the product, you must exclude the folders in your specified installation location.

You can verify the location of these folders by running the MailMarshal SMTP Server Tool from the MailMarshal Tools group in the MailMarshal program group on each Server. Click the Folders tab to see the folder locations. For more information, see “Changing Folder Locations” on page 297.

For information about excluding folders from on-access scanning, refer to your antivirus product documentation. For example, in Network Associates NetShield, you can specify exclusions using the Exclusions tab in Scan Properties.

In your antivirus scanning product control panel, exclude the following MailMarshal SMTP folders from virus scanning:

```
C: \Program Files\Marshal \Mail Marshal \Quarantine  
C: \Program Files\Marshal \Mail Marshal \Queues\Decryption  
C: \Program Files\Marshal \Mail Marshal \Queues\Incoming  
C: \Program Files\Marshal \Mail Marshal \Unpacking
```



MailMarshal SMTP uses folders in the Quarant i ne folder to store messages, including those quarantined by virus scanning rule actions. The product stores email in the Queues\Decrypt i on and Queues\I ncomi ng folders pending processing.

MailMarshal SMTP copies files to the Unpacki ng folder to scan for viruses. If an antivirus scanner finds and cleans a file in the Unpacki ng folder before MailMarshal SMTP scans for viruses, MailMarshal SMTP may determine the file is virus-free and deliver the email with the virus still present.

## Configuring MailMarshal SMTP to Use an Antivirus Product

If you have installed MailMarshal SMTP as an array with more than one Server, you must make the same virus scanners available on all MailMarshal SMTP Servers. You can make a scanner available by installing the software on the MailMarshal SMTP Server, or in some cases by installing the virus scanner software remotely and configuring MailMarshal SMTP to access it.

If you install command line virus software on more than one MailMarshal SMTP Server, you must install it in the same location (same drive letter and folder) on each Server.

### To configure virus scanning in MailMarshal:

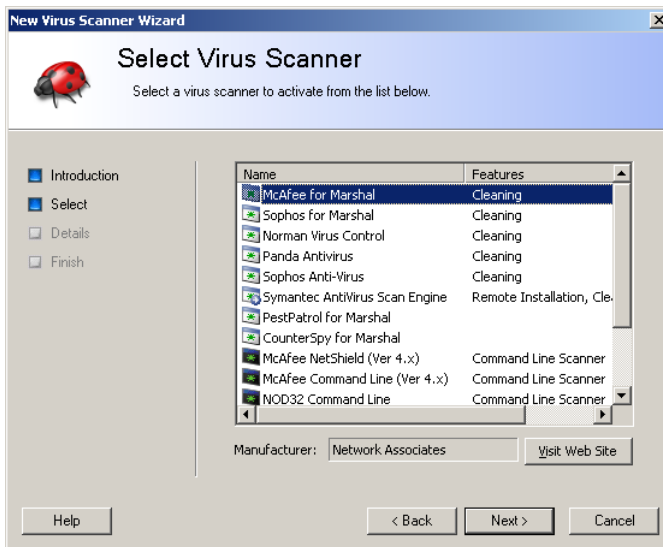
1. Ensure you have installed one or more supported virus scanners on each MailMarshal SMTP Server computer, following the manufacturer's instructions. ***If your antivirus scanner supports remote access***, you can install the scanner in a central location to support several email processing servers.
2. Ensure the scanner does not perform on-demand scanning of the MailMarshal SMTP excluded folders. For more information, see “Excluding Working Folders From Virus Scanning” on page 65.

3. On the MailMarshal SMTP Array Manager computer, run the MailMarshal SMTP Configurator.
4. In the left pane of the Configurator, expand **MailMarshal Configurator > Policy Elements**, and select **Virus Scanners**.
5. On the Action menu, choose **New Virus Scanner**.



**Note:** For detailed guidance on this wizard, click *Help* on each window.

6. On the Welcome window, click **Next**.
7. On the Select a Virus Scanner window, select your antivirus scanner from the list.



8. *If you are configuring a command line scanner*, on the Configure Virus Scanner Path window, specify or browse to identify the location of the antivirus scanner program, such as `c:\McAfee\Scan.exe`.

9. *If the scanner is installed remotely*, on the Configure Virus Scanner Location window enter the server name or IP address and port where the scanner can be accessed.
10. *If your scanner is not in the list*, select **Custom Scanner**. Specify the details of your antivirus software, and then, click **Next**.
11. On the Finish window of the Wizard, click **Finish** to add the virus scanner. MailMarshal SMTP will test the action of the scanner on each installed MailMarshal SMTP email processing server.
12. *If you plan to use more than one virus scanner*, repeat Steps 5 through 11 for each scanner.

## INSTALLING MAILMARSHAL SMTP REPORTS

You can install MailMarshal SMTP Reports on one or more computers in the local network. Each computer must be able to connect to the MailMarshal SMTP database using Named Pipes or TCP (port 1433 by default). For more information about hardware and software requirements and SQL Express licensing limitations, see “Reports User Interface Requirements” on page 34.

### To install MailMarshal SMTP Reports on a workstation:

1. Ensure you have installed all prerequisite software for Reports installation. For more information, see “Reports User Interface Requirements” on page 34.
2. Log on as a local administrator to the computer on which you want to install the MailMarshal SMTP Reports components.
3. Close any open applications.
4. Run the setup program from the MailMarshal SMTP installation kit.
5. On the Setup tab, click **Reports Setup**.

6. On the Welcome window, click **Next**.
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement**, and then click **Next**.
9. Choose an installation folder, and then click **Next**.
10. Review your installation choices and then click **Install**.
11. Ensure **Launch MailMarshal Reports** is selected, and then click **Finish**.
12. On the Database Details window, specify the authentication method and details. For more information, click **Help**.
13. Click **OK**.

For more information about running Reports, see “Generating Reports” on page 320.

## INSTALLING AND CUSTOMIZING WEB COMPONENTS

MailMarshal SMTP includes the following Web-based consoles:

- A Web version of the Console application that allows administrators and others, such as help desk personnel, to view server status and manage quarantined email for all users.
- A Spam Quarantine Management console that allows email recipients to review and manage their own quarantined messages.

You can install the Web Console on Microsoft IIS servers that can connect to the MailMarshal SMTP Array Manager computer on the configuration port (19001 by default). You can also install the Spam Quarantine Management component on a multi-server Web farm using the state management features of ASP.NET.

For more information about hardware and software requirements, see “Web Components Requirements” on page 32.

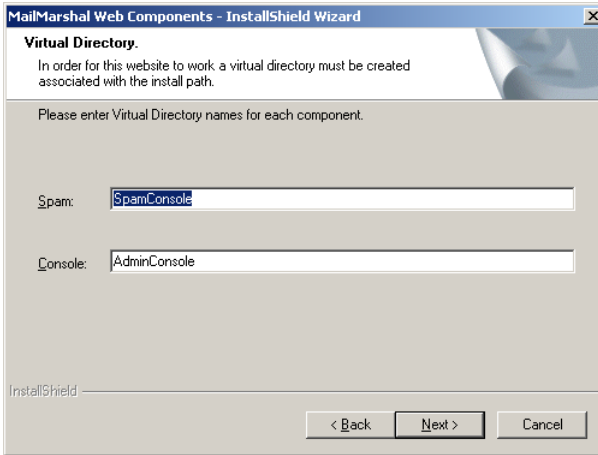
## Installing the MailMarshal SMTP Web Components

Run the Web Components setup to install the MailMarshal SMTP Web Console and Spam Quarantine Management Website.

### To install the Web components:

1. Ensure you have installed all prerequisite software specified for a Web components computer. For more information, see “Web Components Requirements” on page 32.
2. Log on as a local administrator to the computer on which you want to install the MailMarshal SMTP Web components.
3. Close any open applications.
4. Run the setup program from the MailMarshal SMTP installation kit.
5. On the Setup tab, click **Web Components Setup**.
6. On the Welcome window, click **Next**.
7. On the Setup Type window, choose which components you want to install: **Spam Management**, **Web Console**, or **Both**. Click **Next**.
8. On the License Agreement window, carefully read the license information.
9. Click **I accept the terms of the license agreement**, and then click **Next**.
10. Choose a destination location and program folder. By default the location is the C: \Program Files\Marshal folder.

11. On the Virtual Directory window, enter a website directory name for each component you have chosen to install. These names become the virtual path of the site URLs, in the default website on the server.



12. Click **Next**.

13. If you chose to install the Web Console on the same server as the Array Manager, enter the following values on the Web Console Configuration window, and then click **Next**:

- a. Enter the port used by the Array Manager. The default value (19001) is the default port used.
- b. Choose Windows or Forms authentication.



**Note:** If you choose Windows authentication, authorized users will be logged in automatically (Integrated Authentication). If you choose Forms authentication, users can select a server and username each time they log in. For information about how to change authentication methods after installation, see M86 Security Knowledge Base article Q12253.

14. On the Ready to Install the Program window, click **Install**.
15. On the Setup Wizard Complete window, click **Finish**.

16. To complete setup of the Spam Quarantine Management website, run Internet Explorer. The default URL for this site is `http:////SServerName/SpamConsole` where `SServerName` is the name of the Microsoft IIS server where you installed the Web components.
17. On the configuration page of the Spam Quarantine management site, specify the Site URL, Array Manager connection information, User Authentication method, and User Interface settings. For more information, click **Help**.



**Note:** You can set the authentication method for a MailMarshal SMTP installation only once. If you install the Spam Quarantine Management Web component on more than one Microsoft IIS server, all the servers must use the same method.

**MAILMARSHAL**  
Spam Quarantine Management

**Website Address**   
Specifies the URL of the root directory of the MailMarshal Spam Quarantine Management web site. MailMarshal uses this value when it places links in the text of email messages to users, such as digest messages and verification messages.

**Server**   
Specifies the name of the Manager server. Enter a computer name, an IP address, or a fully qualified domain name.

**Port Number**   
Specifies the port that the MailMarshal Manager uses to accept connections. The default value is 19001.

**Username**

**Domain**

**Password**

**Confirm Password**

**Authentication Mode**

**Administrator Email Address**   
This will create a new Administrator User using the given Email Address, and a password will be sent to it.

18. As part of Spam Quarantine managements site setup, the site creates an administrator login (for the specified email address, or the Windows login used to access the configuration page). You can change many site settings later by logging in to the site using the Administrator login.
19. The Web Console does not require any configuration. Each time you connect, you can specify the Array Manager port and account information. The default URL for this site is `http://IISServerName/AdminConsole` where `IISServerName` is the name of the Microsoft IIS server where you installed the Web components.

## Customizing the Web Components

You can configure user interface settings for the Spam Quarantine Management website, using the Administrator login. The configurable settings include:

- Default Theme
- Availability of custom Blocked and Safe Senders lists
- Availability of email address management (add or delete an email address from the list of addresses managed by the user)
- Availability of mail history charts, folder message counts, and the “all folders” view



**Note:** *The charts, counts, and “all folders” view can slow site performance, especially on larger sites. If you are experiencing slow page loading, M86 Security recommends you disable these features.*

Each user can customize their default theme, language, and chart settings (if permitted by the administrator).

The default setup includes two sample themes, and English and Spanish language packs. You can also create new themes and add language packs. For more information about creating your own themes and packs, see M86 Security Knowledge Base article Q11916.



# INSTALLING ADDITIONAL USER INTERFACES

You can install the MailMarshal SMTP Configurator and Console on additional computers to distribute access to the managing and monitoring features the users interfaces provide. The Console communicates with the Array Manager using port 19001. The Configurator also uses NetBIOS ports.

## To install the MailMarshal SMTP Configurator or Console:

1. On the computer where you want to install a user interface, log on with a user account that has permission to access the Array Manager computer.
2. Run the setup program from the MailMarshal SMTP installation kit.
3. On the Setup tab, click **Install MailMarshal SMTP**.
4. On the License Agreement window, carefully read the license information.
5. Click **I accept the terms of the license agreement**, and then click **Next**.
6. On the Setup Type window, choose **Custom Install** then click **Next**.
7. On the Component Selection window, clear **Array Manager** and **SMTP Server**.
8. Select the user interfaces you want to install, and then click **Next**.
9. Specify or browse to a location to install the MailMarshal SMTP files, and then click **Next**.
10. Review your installation choices on the Ready to Install the Program window, and then click **Install**.
11. Ensure **Run the Configuration Wizard** is not selected, and then click **Finish**.

12. On the Connect to MailMarshal Manager window, specify the MailMarshal SMTP Array Manager computer and connection port. By default, the Array Manager uses port 19001.
13. Click **OK**.

## UPGRADING MAILMARSHAL SMTP

You can upgrade MailMarshal SMTP to the latest version. Depending on which version you have currently installed, the required procedures differ. Be sure to read the release notes for any version-specific information.

### Upgrading from MailMarshal SMTP Version 6.4.5 or Above

You can upgrade to the latest release of MailMarshal SMTP from MailMarshal SMTP 6.4.5 or later versions. Upgrade the Array Manager first. Then upgrade other MailMarshal SMTP components.



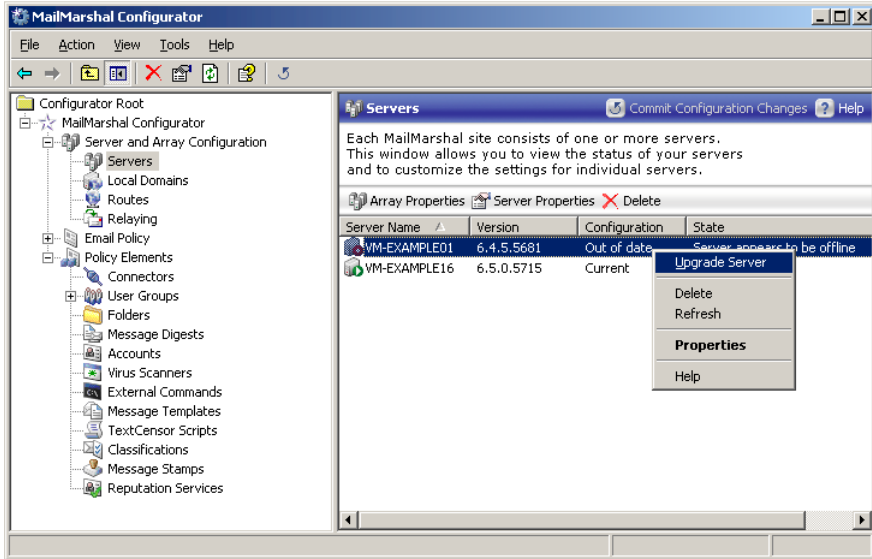
**Note:** To upgrade from earlier versions, first upgrade to 6.4.5 or above (6.7 is recommended and provided on the M86 Security website).

#### To upgrade to the latest version of MailMarshal SMTP:

1. Ensure the computer you want to upgrade meets the prerequisites for the latest version of MailMarshal SMTP.
2. Ensure you update Microsoft SQL Server to a supported version before you continue. For more information, see “Hardware and Software Requirements” on page 26.
3. Log on as a local administrator to the MailMarshal Array Manager computer.


4. Run the MailMarshal SMTP Configurator from the MailMarshal Program group.
5. Back up your MailMarshal SMTP configuration. For more information, see “Backing Up the Configuration” on page 261.
6. Close the MailMarshal SMTP Configurator.
7. Run the MailMarshal SMTP setup program from the CD or Web distribution.
8. On the Setup tab, click **Install MailMarshal SMTP**.
9. On the Welcome window, the setup program displays the current version of MailMarshal SMTP and the version to which it will upgrade. Click **Next**.
10. On the License Agreement window, carefully read the license information.
11. Click **I accept the terms of the license agreement**, and then click **Next**.
12. On the Ready to Install window, click **Install**. The setup program stops the MailMarshal SMTP services, updates the product files and database, and restarts the services.
13. On the Update Complete window, click **Finish**.
14. ***If you are upgrading a MailMarshal SMTP Array:***
  - You can upgrade processing servers remotely as described in this step. To upgrade processing servers manually, see Step 15.
  - a. After upgrading the Array Manager, run the Configurator.
  - b. In the left pane, select Server and Array Configuration.

- c. In the right pane, right click a server entry in the list and select **Upgrade Server**. The server will be upgraded and restarted automatically.



- d. Repeat step c for each server entry

- e. Continue with Step 16.

 **Note:** After you upgrade the Array Manager, the servers may show as “offline” in the Configurator for a few minutes. However, email continues to flow.

- The remote server upgrade process copies the required software to the target server, stops email processing on the target server, installs the new software, and restarts the target server. This process typically takes a few minutes to complete.

**15. To upgrade processing servers manually:**

- a. On a MailMarshal SMTP Server computer, run the setup program from the CD or Web distribution and complete the upgrade process.
  - b. When the upgrade process is complete, specify the name of the MailMarshal SMTP Array Manager computer and port over which to connect.
  - c. Repeat Steps **a** and **b** on each MailMarshal SMTP Server computer.
- 16.** On the MailMarshal SMTP Array Manager computer run the Configurator to verify that each email Server is connected and to ensure the Receiver, Engine, and Sender services are running.

**17. If you are using the MailMarshal SMTP Web components:**

- a. **If you have customized any Web component graphics**, make a backup copy of the custom files to a backup folder. For more information, see “Customizing the Web Components” on page 74.
- b. On the Web components computer, run the MailMarshal SMTP setup program from the CD or Web distribution.
- c. On the Setup tab, click **Install Web Components**.
- d. Run the Web components setup until you have completed the installation process.
- e. **If you backed up custom graphic files**, copy your backup files to the proper locations in the new install folders.

**18. If you are using Reports:**

- a. On the computer where you install Reports, run the MailMarshal SMTP setup program from the CD or Web distribution.
- b. On the Setup tab, click **Install MailMarshal Reports**.
- c. Continue running the Reports setup until you have completed the installation process.

19. Refer to the Release Notes to learn more about new product features and updates. For more information about using the new version of the product, see the *User Guide*.

## Upgrading from Other Versions of MailMarshal SMTP

**To upgrade from MailMarshal Version 6.2 or below:**

1. First upgrade to MailMarshal SMTP 6.4 (or earlier 6.X version).

**Note:** Before upgrading from version 6.0 or version 6.1.3, see additional version-specific upgrade information available in M86 Security Knowledge Base articles Q11026 and Q11027.

2. Then upgrade again to the current version of MailMarshal SMTP.

There are several important steps to this process. For more information about upgrading from MailMarshal Version 5.5 SMTP, refer to the “Upgrading MailMarshal SMTP 5.5 Installations to MailMarshal SMTP 6.X” technical reference, available at [www.m86security.com](http://www.m86security.com). Additional information is available in M86 Security Knowledge Base article Q11025.

MailMarshal SMTP no longer supports the integrated MailMarshal Secure package (S/MIME). To upgrade from MailMarshal Version 5.5 SMTP using MailMarshal Secure, you must remove the MailMarshal Secure component by running the Add/Remove Programs application in Windows Control Panel.

If you want to continue using S/MIME, you can use the MailMarshal Secure Email Server solution, available separately from M86 Security.

MailMarshal now includes Transport Layer Security (TLS), which may provide an alternate security solution for your organization. For more information about TLS, see “Securing Email Communications” on page 289.

To remove the MailMarshal Secure component from a MailMarshal Version 4.2.5 SMTP installation, first upgrade to MailMarshal Version 5.5 SMTP. Then, remove the MailMarshal Secure component using Add/Remove Programs. Continue to follow the upgrade process for MailMarshal Version 5.5 SMTP.

## UNINSTALLING MAILMARSHAL SMTP

If you choose to uninstall MailMarshal SMTP, you must reroute your email to suit your new configuration. The following steps provide guidelines for the types of steps you must take to remove MailMarshal SMTP from your email delivery mechanisms.

When you uninstall MailMarshal SMTP, you will no longer be able to use the MailMarshal SMTP Console to view the contents of the Quarantine folder on the server.

### To uninstall MailMarshal SMTP:

1. Run the MailMarshal Configurator.
2. In the left pane, expand **MailMarshal Configurator > Servers and Array Configuration**.
3. In the right pane, select the Server you wish to uninstall.
4. Click the **Properties** icon in the Configurator toolbar or **Server Properties** in the task pad toolbar.
5. Select the **Receiver** service, and then click **Stop**.
6. Click **OK**.

7. Allow the Engine and Sender services to run until MailMarshal SMTP processes all the received email. You can verify that all mail queues are empty by running the MailMarshal Console.
8. Reroute your email delivery settings to exclude the MailMarshal SMTP Server you want to uninstall. For example, you may need to change the DNS MX records, firewall translation settings, and internal email server settings that directed email to the MailMarshal SMTP server both from external email and from your internal email server.
9. Verify that email is flowing through the new path and no email is being delivered to the MailMarshal SMTP server you plan to uninstall.
10. ***If you want to preserve the data from the MailMarshal Server you are uninstalling***, back up the contents of the MailMarshal SMTP Quarantine folder and all subfolders.
11. Run Add/Remove Programs in Control Panel to remove MailMarshal. You may have to restart your computer to remove some program files.
12. To delete the Quarantine folders, first delete the contents of the Symbolic subfolder.
13. Delete the remaining Quarantine folders and files.
14. *If you are uninstalling one email processing server but continuing to use MailMarshal SMTP:*
  - a. On the Array Manager computer, run the MailMarshal Configurator.
  - b. In the left pane, expand **MailMarshal Configurator > Server and Array Configuration**.
  - c. In the right pane, select the server you uninstalled.
  - d. Click the **Delete** icon on the Configurator or task pad toolbar.
15. ***If you are using a MailMarshal SMTP array and want to remove the product completely***, repeat Steps 1 through 14 on each additional email processing server.



- 16.** Use Add/Remove Programs from the Windows Control Panel to remove additional components you may have installed, such as Web components or Reports.
- 17.** Uninstall additional instances of the Console on each computer where it is installed.
- 18.** Use Add/Remove programs from the Windows Control Panel to remove the MailMarshal Configurator.



---

## Chapter 4

# Understanding MailMarshal SMTP Interfaces

MailMarshal SMTP provides several interfaces to help you set up and monitor email content security.

### **MailMarshal SMTP Configurator**

Allows you to customize your content security policy, configure email delivery options, and control user access to other consoles.

### **MailMarshal SMTP Console**

Allows you to monitor server health and email traffic flow on a real-time basis, and manage quarantined email messages. Also provides access to support news and updates from M86 Security.

### **MailMarshal SMTP Web Console**

Provides most features of the MailMarshal SMTP Console through a Web interface.

### **MailMarshal SMTP Reports Console**

Allows you to generate detailed historical reports on email traffic, policy breaches, and MailMarshal SMTP actions.

### **MailMarshal SMTP Spam Quarantine Management Website**

Allows email users to review and unblock email that MailMarshal SMTP has quarantined as spam, and to maintain lists of safe and blocked senders. You can also configure this site to give users the same powers over any quarantine folder.

### **Other Tools**

Provide access to setup of items that cannot be changed within the main interfaces. The tools include a server setup tool, and command line tools to import user and group information and configuration from files.

# UNDERSTANDING THE CONFIGURATOR

The MailMarshal SMTP Configurator (Configurator) uses Microsoft Management Console (MMC) technology. The Configurator is always installed on a standalone MailMarshal SMTP server, or on the Array Manager server when you install a MailMarshal SMTP array. You can also install the Configurator on other workstations within your LAN. Only one Configurator can be connected to the server at a time.



**Note:** *So that MailMarshal SMTP can detect and block email with explicit language, such as profanity and pornographic language, the Email Policy rules and the TextCensor scripts must contain that explicit language. Anyone with permission to run the MailMarshal Configurator may be exposed to this explicit language. Since this language may be objectionable, please follow your company's policy about employee exposure to potentially objectionable content.*

The left pane of the Configurator is the menu pane. The right pane of the Configurator is the details or results pane. When you select an item in the left pane, the right pane changes to reflect details for that item. The right pane defaults to a taskpad view in most cases. In the taskpad view, MailMarshal SMTP displays shortcuts to common tasks at the top of the pane.

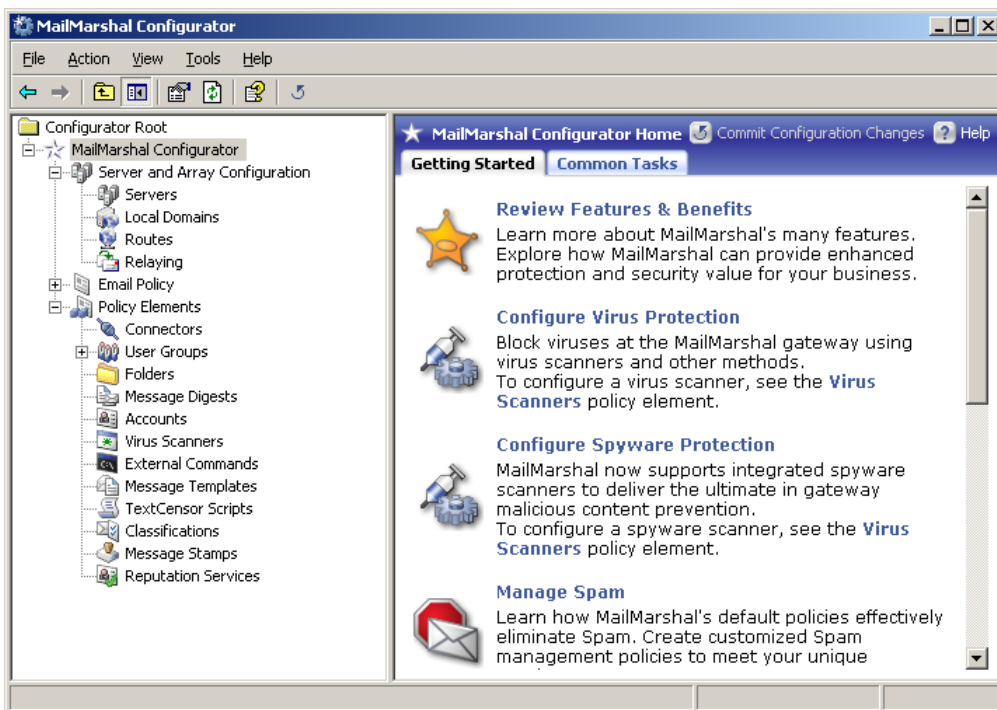


**Note:** *Many items in the Configurator include a right-click menu that lets you choose context-sensitive actions. The items on right-click menus are also available on the menus, the toolbar and/or the taskpad for the selected item.*

To start the Configurator, click **MailMarshal Configurator** in the MailMarshal SMTP program group.

## Working With the Getting Started and Common Tasks Pages

When you start the Configurator for the first time, the right pane shows a taskpad with two tabs: Getting Started and Common Tasks. You can return to this view by clicking **MailMarshal Configurator** in the left pane. The items on these tabs provide guidance on selected important features of MailMarshal SMTP.



Click the title of any item to read additional information about what the feature does and how to use it. Click the additional link in the body of some items to open the user interface for the feature.

## Working With Menu and Detail Items

Expand the menu in the left pane by clicking the + symbol to the left of an item. View the list of detail items for a menu item by clicking the menu item. View detailed properties of an item by selecting it and then clicking the **Properties** icon in the toolbar.



**Note:** You can export most lists of detail items (such as users or folders) to a file, by using the MMC Export List function. To use Export List, right-click the item in the left pane and select **Export List**, or select the item and use the Action menu.

## Working With Properties Configuration

You can set many global properties of MailMarshal SMTP using two properties windows.

### MailMarshal Properties

This window allows you to configure basic properties of the MailMarshal SMTP installation. You can also back up or restore a MailMarshal SMTP configuration. You can control how MailMarshal SMTP receives and delivers email and you can also set up some email filtering that will be applied to all messages. To open this window, on the Tools menu select **MailMarshal Properties**. **To view and change specific settings**, select an item from the menu tree at the left of the Properties window.

### Node Properties

Each MailMarshal SMTP installation includes one or more email processing servers, also known as nodes. To see a list of these servers, click **Server and Array Configuration** in the left pane of the Configurator. The right pane displays a list of installed servers. To configure settings for a server, click to select that server in the right pane, then click the **Server Properties** icon in the toolbar. **To view and change specific settings**, select an item from the menu tree at the left of the Properties window.

For more information about the properties and settings shown on these windows, see “Configuring Email Content Security” on page 97 and “Managing Array Nodes” on page 282

## Committing Configuration

Changes you make to the MailMarshal SMTP configuration are not applied to email processing servers immediately. **To apply the changes**, on the Tools menu choose **Commit Configuration**.

If configuration has not been committed, the status bar at the lower right of the MMC indicates **Reload required** or **Restart required**, and the caption **MailMarshal Configurator** at the top of the left pane of the Configurator is followed by the symbol **-\*** (reload required) or **-!** (restart required). “Restart required” indicates that the MailMarshal SMTP services on email processing servers will restart when the new configuration is applied.

If you have configured “commit scheduling,” then committing configuration might not apply the configuration to the email processing servers immediately. If the configuration has not been applied, the status bar at the lower right of the MMC indicates **Update pending**. For more information about commit scheduling, see Help for MailMarshal Properties > Commit Scheduling.

To check whether the email processing servers are up to date with the latest configuration you have committed, in the left pane of the Configurator click **Server and Array Configuration**. The status of each server shows **Current** if the server is up to date. To force an immediate update of the server configuration, right-click the server name and select **Deploy configuration**.

# UNDERSTANDING THE CONSOLE

The MailMarshal SMTP Console (Console) uses MMC technology. The Console is always installed on a standalone MailMarshal SMTP server, or on the Array Manager server and each email processing node when you install a MailMarshal SMTP array. The Console can also be installed on other workstations within the LAN.

The right pane of the Console is the details or results pane. When you select an item in the left pane, the right pane changes to reflect details for that item. The right pane defaults to a taskpad view in most cases.

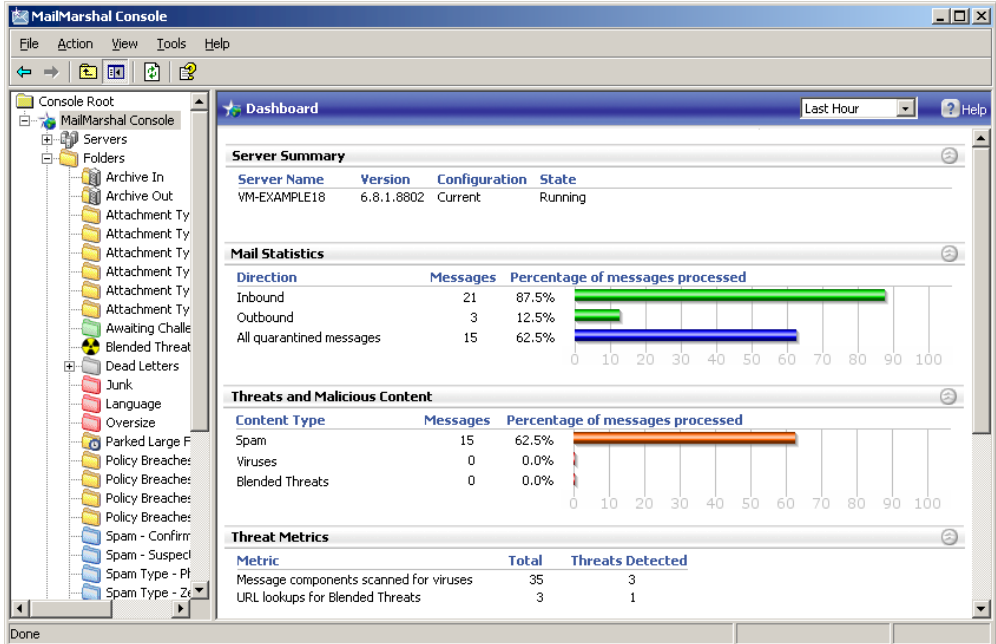


**Note:** *Many items in the Console include a right-click menu that lets you choose context-sensitive actions. The items on right-click menus are also available on the toolbar and/or the taskpad for the selected item.*

*You can export most lists of detail items (such as folder contents, Mail History or history search results) to a file, by using the MMC Export List function. To use Export List, right-click the item in the left pane and select **Export List**, or select the item and use the Action menu.*



To start the Console, click **MailMarshal Console** in the MailMarshal SMTP program group. The Console displays a quick overview of server health and statistics.



The Console also provides access to support news and updates from M86 Security, using RSS feeds from the M86 Security website. You will be notified of the most important new items each time you open the Console.

For more information about the features and functions of the Console, see “Using the MailMarshal SMTP Console” on page 231.

## UNDERSTANDING THE WEB CONSOLE

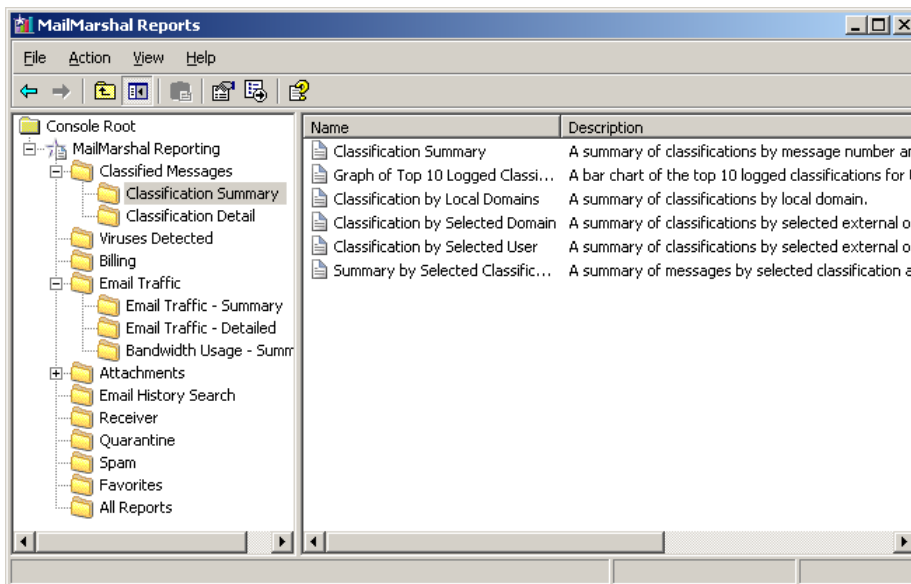
The MailMarshal SMTP Web Console (Web Console) uses Microsoft Internet Information Services (IIS). The Web Console can be installed on any Microsoft IIS 5.0 or higher server that can connect to the MailMarshal SMTP Array Manager or standalone MailMarshal SMTP server.

The Web Console provides most functions of the MailMarshal SMTP Console. It supports Microsoft Internet Explorer version 5.5 and higher. The browser must be configured to use JavaScript and to accept cookies. You may also be able to use the Web Console with recent versions of other Web browsers.

For more information about the features and functions of the Web Console, see “Using the MailMarshal SMTP Console” on page 231.

# UNDERSTANDING THE REPORTS CONSOLE

MailMarshal SMTP Reports can be installed on any workstation that can connect to the MailMarshal SMTP database. To start MailMarshal SMTP Reports, click **MailMarshal Reports** in the MailMarshal SMTP program group. The Reports interface gathers the available reports into folders.



For more information about the features and functions of the Reports Console, see “Generating Reports” on page 320.

MailMarshal SMTP customers can also install the Marshal Reporting Console. The Marshal Reporting Console uses SQL Server Reporting Services to provide web-based delivery and scheduling of reports. For more information, see the documentation on Marshal Reporting Console.

# UNDERSTANDING THE SPAM QUARANTINE MANAGEMENT WEBSITE

The MailMarshal SMTP Spam Quarantine Management Website (Spam Console) uses Microsoft IIS. The Spam Console can be installed on any Microsoft IIS 5.0 or higher server that can connect to the MailMarshal SMTP server or Array Manager. It supports Microsoft Internet Explorer version 6.0 and higher. The browser must be configured to use JavaScript and to accept cookies. The Spam Console allows users to see a summary of blocked mail, release messages, and manage a variety of settings.

The screenshot displays the MailMarshal Spam Quarantine Management website. The browser title is "MailMarshal SQM - Home - Microsoft Internet Explorer provided by Marshal Software Ltd". The address bar shows "http://vm-example16/SpamConsole/Default.aspx". The user is logged in as "VM-EXAMPLE16\User".

The main content area includes a navigation menu with "Home", "Blocked Mail", "Manage Senders", and "User Settings". A search bar is labeled "Mail Search". A welcome message says "Welcome VM-EXAMPLE16\User" and "You have 3 new blocked emails".

Under "Blocked Spam", there are three pie charts:

- Today's Data:** Allowed 0 (0%), Blocked 3 (100%), Total 3.
- This Week's Data:** Allowed 2 (28%), Blocked 5 (71%), Total 7.
- This Month's Data:** Allowed 2 (28%), Blocked 5 (71%), Total 7.

Below the charts is the "Latest Blocked Mail" section with buttons for "Unblock", "Safe Sender", "Block Sender", and "Delete". A table lists the blocked mail items:

<input type="checkbox"/>	From	Subject	Size	Date
<input type="checkbox"/>	jack@somedomain.com	R()!e><	1243	1:33 p.m.
<input type="checkbox"/>	jack@somerandomdomain.com	Bop till you drop	985	1:32 p.m.
<input type="checkbox"/>	jack@somerandomdomain.com	shop till you drop	559	1:32 p.m.

At the bottom, there is a "View All" button and footer information: "Home | Blocked Mail | Manage Senders | User Settings", "© 1990 - 2010 M86 Security, www.m86security.com", "MailMarshal SQM Version: 6.0.1.8848", and "Array Manager Version: 6.0.1.8848".

# UNDERSTANDING OTHER TOOLS

The **MailMarshal Server Tool** allows you to change various settings related to communication between the MailMarshal SMTP server(s) and the MailMarshal SMTP database. These settings cannot be changed from within other interfaces for technical reasons.

The **Group File Import Tool** allows you to import user and group information into MailMarshal SMTP user groups from a text file. For more information, see “Using the Group File Import Tool” on page 298.

The **Configuration Export Tool** allows you to import and export MailMarshal SMTP configuration information from a command line or batch file. For more information, see “Using the Configuration Export Tool” on page 300.

In Appliance installations, the **appliance Web interface** (NEWS interface) allows you to configure, monitor, and manage a node appliance. For more information, see the *Appliance Administrator Guide*.



---

## Chapter 5

# Implementing Your Email Content Security Policy

MailMarshal SMTP provides a powerful and flexible framework that allows you to enforce an Email Content Security policy. Configure MailMarshal SMTP to support your organizational Acceptable Use Policy for email usage.

An Email Content Security policy typically has several goals:

- To stop spam.
- To block virus infected email.
- To prevent illegitimate relaying of email.
- To control who can send email through your server.
- To prevent malicious email attacks
- To filter email messages and attachments according to local policies of the organization.

MailMarshal SMTP includes facilities to perform these tasks. MailMarshal SMTP is configured by default with settings and rules that implement some best practices and common filtering policies out of the box. This chapter gives an overview of typical policies and policy-related tasks, and the MailMarshal SMTP elements available to accomplish each task.

## CONFIGURING EMAIL CONTENT SECURITY

Configure email content security using the MailMarshal SMTP Configurator. For basic information about the Configurator see “Understanding the Configurator” on page 86

Content Security policies generally include elements of two types:

### **Email transport policies**

These policies are implemented using global settings you configure in **MailMarshal Properties**. These policies control who is allowed to send email to or through the MailMarshal SMTP server. For more information on email transport policies, see “Configuring SpamProfiler” on page 101, “Preventing Relaying” on page 109 and “Controlling Who Can Send Email Through Your Server” on page 111.

### **Email content policies**

These policies are implemented using rules you configure as part of MailMarshal SMTP Email Policy. These policies control the content of email messages. For more information on email content policies, see “Stopping Spam” on page 98, “Stopping Viruses” on page 105, and “Filtering Messages and Attachments” on page 124.

To work with the Configurator, click **MailMarshal Configurator** in the MailMarshal program group.

## **STOPPING SPAM**

Stopping unsolicited incoming email (commonly known as spam) is a primary goal for most organizations. The M86 Security SpamCensor and SpamBotCensor technology filter spam efficiently with minimal overhead. The SpamProfiler is a signature based check performed at the Receiver, that allows MailMarshal to refuse delivery of spam or quarantine it with minimal processing.

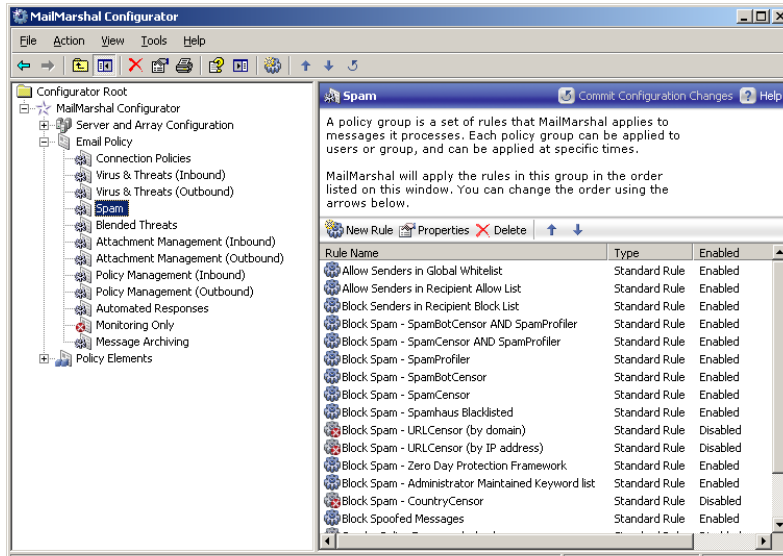
## **Spam Configuration and Rules**

The default email policy provided with MailMarshal SMTP includes a policy group titled Spam. This policy group includes a number of rules to block spam. Some basic rules are enabled by default. Additional rules can be enabled and/or customized to suit each installation.



## To view the Spam policy group:

1. In the left pane of the Configurator, expand the item **Email Policy**.
2. Expand the item **Spam**.



3. View details of each rule, including a description of its intended use, by selecting the rule in the right pane and choosing **Properties** from the toolbar of the MMC or the taskpad.

The default rules include:

- Rules to quarantine spam using the SpamBotCensor, SpamCensor and SpamProfiler.



**Note:** To ensure the reliability of SpamCensor and SpamProfiler, verify that they are enabled and correctly configured. See “Configuring SpamProfiler” on page 101 and “Configuring SpamCensor and SpamProfiler Updates” on page 102.

- To ensure the reliability of SpamBotCensor, ensure the processing nodes receive connections directly from the Internet.
- A rule to allow email messages from specific addresses.
- Rules to implement lists of blocked senders and safe senders for each user. Users can update these lists through the MailMarshal SMTP Spam Quarantine Management Website.
- A Zero Day Protection rule that helps to block specific outbreaks, using automatic updates from M86 Security.
- A rule to quarantine email messages that contain specific text, using the MailMarshal SMTP TextCensor.
- A rule to blacklist senders of spam email that contains URLs in the message header or body. The rule uses the URLEncensor function to compare URLs in received messages with blacklists maintained by external blacklist sites. URLEncensor decodes URLs intentionally obscured with decimal, octal, or hexadecimal notation. For more information about using URLEncensor, see the M86 Security Knowledge Base.



**Note:** To use URLEncensor, you must ensure that MailMarshal SMTP uses a reliable, efficient DNS server. For more information, see “Configuring Default Delivery Options” on page 276.

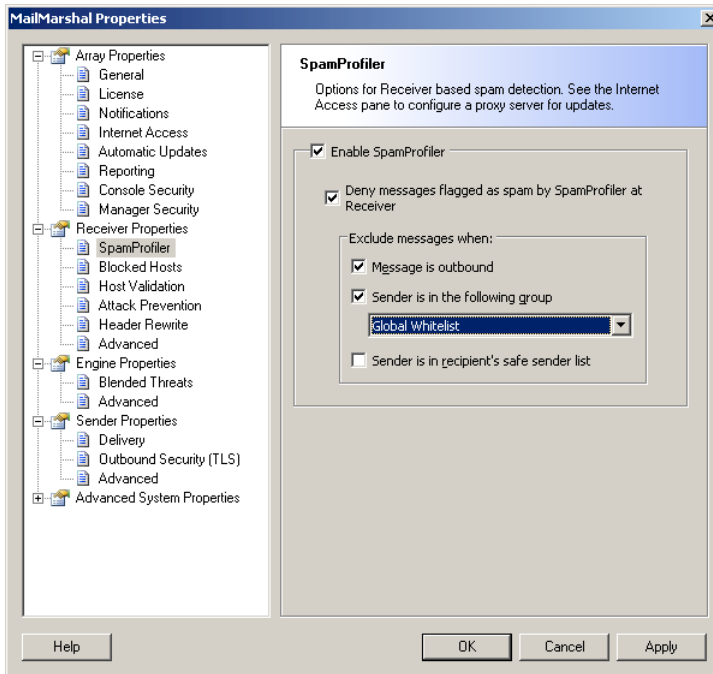
## Configuring SpamProfiler

SpamProfiler is a signature based service that examines email at the MailMarshal Receiver. SpamProfiler can significantly reduce the load on the MailMarshal Engine. By default MailMarshal SMTP enables SpamProfiler and uses Standard Rules to quarantine messages in a folder. You can also use this facility to block messages at the receiver, without unpacking them.

### To configure SpamProfiler:

1. In the Configurator, select **MailMarshal Properties** from the Tools menu.
2. To enable **SpamProfiler**, select it from the left pane and check the box **Enable SpamProfiler**.

3. To block message at the receiver, select the option **Deny messages**. You can exclude groups of senders from blocking using the additional options. For details of the options, see Help.



4. To quarantine or delete messages, enable SpamProfiler and then use the Standard rule condition **Where message is detected as spam by SpamEngine**. For more information see “Where message is detected as spam by SpamEngine” on page 135.

## Configuring SpamCensor and SpamProfiler Updates

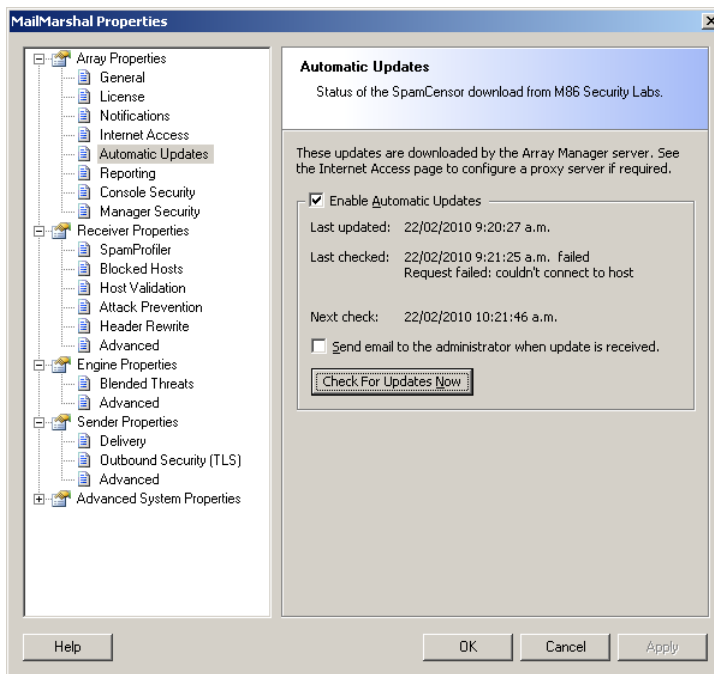
M86 Security provides updates for the SpamCensor and SpamProfiler facilities to all customers with current MailMarshal SMTP maintenance contracts. The updates are delivered through the Web by HTTP and HTTPS.

## Configuring and Checking Automatic SpamCensor Updates

Automatic updating of the SpamCensor is enabled by default. You can choose to download updates manually or automatically.

### To monitor and configure SpamCensor updates:

1. In the Configurator, select **MailMarshal Properties** from the Tools menu.
2. Select **Automatic Updates** from the left pane. The display shows the time and result of the last update attempt, and the time of the next attempt.



3. *If you do not want the SpamCensor to update automatically*, clear the check box **Enable Automatic Updates**.

- 4. If you want to be notified by email when a SpamCensor update is received**, select the check box **Send email to the administrator**.

MailMarshal SMTP sends an email message to the administrator address configured on the Notifications page of MailMarshal Properties.

- 5. If you want to perform a check for SpamCensor updates immediately**, click **Check for Updates Now**.

## ***Configuring Proxy Settings for Updates***

If the MailMarshal SMTP server(s) do not have direct access to the Web, you can configure MailMarshal SMTP to use a proxy server to download the updates. This proxy server setting applies to SpamCensor, SpamProfiler, and Blended Threats Module updates.

SpamCensor updates are downloaded by the Array Manager. SpamProfiler and Blended Threats Module updates are downloaded by each processing node.

### **To configure proxy settings for the updates:**

1. In the Configurator, select **MailMarshal Properties** from the Tools menu.
2. Select **Internet Access** from the left pane.
3. You can configure the following settings for the Array Manager (SpamCensor updates) and for the processing nodes (Blended Threats Module and SpamProfiler updates).
  - a. If you want MailMarshal SMTP to access the Web directly**, select **Direct Access**.
  - b. If you want MailMarshal SMTP to use a specific proxy server**, select **Proxy**. Enter a proxy server name and port. If necessary, enter a user name and password for proxy authentication.
4. To apply the proxy settings, click **OK** to go back to MailMarshal Properties and then commit MailMarshal SMTP configuration changes.

You can also configure different proxy settings for each processing node if necessary. For more information, see “Customizing Settings for Nodes” on page 286.

## STOPPING VIRUSES

Blocking virus infections at the email gateway is a primary goal of email content security for most organizations. MailMarshal SMTP can scan email messages for virus infection using any of a number of virus scanners, including McAfee for Marshal and Norman Antivirus. Nearly all MailMarshal SMTP installations use virus scanning.

MailMarshal SMTP can use one or more scanners to check email for viruses. Because virus scanners have differing architecture and update policies, some organizations choose to use multiple scanners.



**Note:** Before MailMarshal SMTP can use a virus scanner in email processing, you must configure it within MailMarshal SMTP.

For more information about configuring virus scanners, see “Configuring Antivirus Scanning” on page 65.



**Note:** Anti-spyware scanning (*PestPatrol* for Marshal and *CounterSpy* for Marshal) can also be implemented using the same methods. For more information about the value of anti-spyware scanning, see “Anti-Spyware Scanners” on page 340.

## How MailMarshal SMTP Uses Virus Scanners

MailMarshal SMTP invokes the virus scanner after unpacking all elements of an email message. MailMarshal SMTP then passes the elements to the scanner software for analysis, and takes action based on the result returned from the scanner.

## Features

MailMarshal SMTP supports the following virus prevention and management features:

- **Email antivirus scanning at the gateway:** Adds a proactive layer of defense at a key strategic point in the network.
- **Multiple virus and malware scanners (optional):** Increases the chances of detecting a virus and reduces the vulnerabilities from delays in patch updates.



**Note:** Appliance installations are pre-configured using McAfee for Marshal. Appliance installations cannot currently use other scanners.

- **Virus Cleaning (optional):** Allows problem email to be cleared through to the recipient automatically.



**Notes:** Cleaning is available only with DLL based scanners. For more information about scanner capabilities, see M86 Security Knowledge Base article Q10923.

- *The cleaning option is not enabled in default rules. You can modify or add a rule to enable cleaning. For more information, see “To Set Up Virus Cleaning” on page 138.*
- **Virus notification and reporting:** Provides email notifications of specific viruses, and comprehensive reporting on virus incidents (including the virus names if provided by the scanner in use).

MailMarshal SMTP also provides additional features that can help with virus protection, including:

- Unpacking documents and archives
- Scanning text for keywords and suspect code
- Blocking dangerous file types
- Blocking encrypted files



## ***Implementation Options***

To work with MailMarshal SMTP, a virus scanner must have a command-line interface or a MailMarshal SMTP DLL supplied by M86 Security. The scanner must return a documented response indicating whether or not a virus is detected. Most commercially available virus scanners meet these specifications.



**Note:** *Because DLL based scanners are always resident in memory, they are about 10 times faster than command line scanners. M86 Security recommends the use of DLL scanners for sites with high message traffic.*

Install one or more chosen scanners on each MailMarshal SMTP email processing server (or remotely, if the scanner supports remote access) following the manufacturer's instructions. For more information about supported antivirus software, see “Supported Antivirus Software” on page 38. For more information about installing virus scanners, see “Configuring Antivirus Scanning” on page 65



**Tip:** *McAfee for Marshal requires installation of the McAfee for Marshal Console. This software is available on the MailMarshal SMTP CD-ROM, or in a separate download from [www.m86security.com](http://www.m86security.com).*

## **Virus and Threats Policy and Rules**

The default email policy provided with MailMarshal SMTP includes two policy groups titled Virus & Threats (Inbound) and Virus & Threats (Outbound). These policy group include a number of rules to block viruses.

**To view the Virus & Threats policy groups:**

1. In the left pane of the Configurator, expand the item **Email Policy**.
2. Expand the item **Virus & Threats (Inbound)** or **Virus & Threats (Outbound)**.
3. View details of each rule, including a description of its intended use, by selecting the rule in the right pane and choosing **Properties** from the toolbar of the MMC or the taskpad.

The default rules include rules to attempt to block virus infected email messages, to block known virus-related messages by their content, and to implement Zero Day protection.

The rules that invoke virus scanners are disabled by default. You must install and configure at least one virus scanner before you can enable these rules. Before you can configure and enable rules that use the “cleaning” functions, you must install and configure a scanner that supports cleaning.

## Best Practices

M86 Security recommends the following basic practices to ensure security with respect to viruses and virus scanning:

- Block messages and attachments that MailMarshal SMTP cannot scan, such as password protected attachments and encrypted attachments (for example files of type ‘Encrypted Word Document’).
- Block encrypted messages that MailMarshal SMTP cannot decrypt, such as PGP and S/MIME messages and encrypted ZIP files.

- Block executable and script files by type and name. This helps to ensure that unknown viruses will not be passed through.
- Subscribe to email notification lists for virus outbreaks. Such lists are available from many antivirus software companies. When an outbreak occurs, block the offending messages by subject line or other identifying features



**Note:** *If resident or “on access” virus scanning is enabled, exclude the MailMarshal SMTP working folders from scanning. See “Excluding Working Folders From Virus Scanning” on page 65.*

## Viewing Virus Scanner Properties

Double click the name of any virus scanner in the right pane to review and change the MailMarshal SMTP configuration information for that scanner. The fields shown will vary depending on whether the scanner is a command line or DLL based scanner. For details of the fields, see the Help for this window.

## PREVENTING RELAYING

**Relaying** email means sending a message to an email server for delivery to another email server. An **open relay** is an email server that accepts messages from any server for delivery to any other server. Spam senders often exploit open relays. It is best practice for an email server to refuse relaying requests, unless the source is known and trusted.

By default MailMarshal SMTP only allows relaying requests from the email server that was selected for delivery of local email (in the Configuration Wizard). For instance, if you entered the IP address of an Exchange server as the local delivery location, MailMarshal SMTP will also relay outgoing email from the Exchange server.

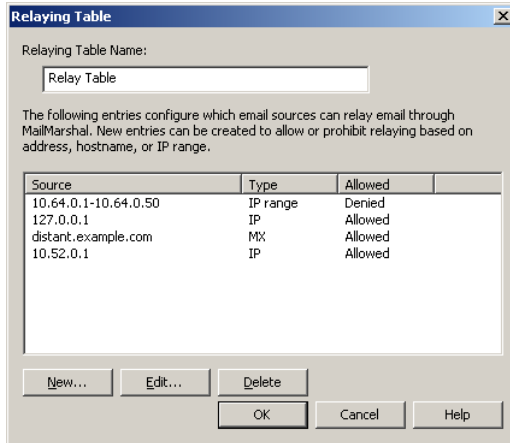
You may need to allow relaying from other locations. You can allow relaying in two ways:

- By specific account authentication. See “Authentication by Account” on page 116.
- By Relaying Table.

**To permit relaying from other locations:**

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration > Relaying**.
2. In the right pane, double-click the default Relaying Table entry. The Relaying Table window displays the list of sources allowed or denied relay permission.
3. To permit relaying from additional computers, click **New**.

4. In the Configure Relaying Address window select one of the available options, and then enter the required data. For example, you can choose to permit relaying from the IP range 10.15.1.0 - 10.15.1.255.



5. Click **OK** to both windows, and then commit configuration changes.



**Notes:** For more details of the available options, see “Configuring Relaying” on page 273. For details of the fields on the windows, click *Help*.

- To learn about an additional item that affects relaying in rare cases, see *Help* for the setting “Block suspicious local-part relay attempt.”

## CONTROLLING WHO CAN SEND EMAIL THROUGH YOUR SERVER

MailMarshal SMTP includes a number of features that allow you to control acceptance of email messages. These include Reputation Service checking, PTR lookups, a list of blocked hosts, and authentication by account (user name and password).

## Reputation Services and DNS Blacklists

MailMarshal SMTP can retrieve information from Reputation Services or DNS based blacklists including the Marshal IP Reputation Service, and third-party services such as SpamCop and SpamHaus. A **Reputation Service** is a service that provides an automated response through the DNS protocol. These services typically attempt to list email servers that are associated with spamming, open relays, or other unacceptable behavior. Each list has its own policies, and you should carefully evaluate the lists you choose to use.

Configuring a Reputation Service for use in MailMarshal SMTP is a two step process. You configure details of the service in Policy Elements, and then you configure one or more receiver rules to filter email based on the list information.

### ***Recommended Usage***

To minimize performance issues, use only one or two reliable services.

You can view the result returned by a Receiver rule Reputation Service condition by reviewing the MailMarshal SMTP Receiver text log.



**Note:** MailMarshal SMTP improves Reputation Service performance by automatically maintaining a list of trusted IP addresses (“automatic adaptive whitelisting”). Connections from servers on this list are not submitted for checking. The list of trusted addresses is generated based on recent server activity, using a proprietary heuristic. You can choose to enable or disable adaptive whitelisting for each Reputation Service that you configure.

- You can also use reputation services in standard rules through the MailMarshal SMTP Category (Spam Censor) facility. This is a more flexible method because it allows for weighted combinations of conditions. For more information about this facility, see the white paper “MailMarshal SMTP Anti-Spam Configuration,” available from the M86 Security website. You can view the result returned by a Category reputation service lookup in the message log (if the message is quarantined) or the MailMarshal SMTP Engine text log.

## ***Configuring Access to a Reputation Service***

MailMarshal SMTP maintains a list of available reputation services it can use in Receiver rules.

### **To configure access to a reputation service:**

1. In the Configurator, expand **Policy Elements > Reputation Services**. The right pane shows a list of configured services.
2. You can edit a service entry or add a new entry. See Help for details of the required information.



**Notes:** *The Marshal IP Reputation Service is available for use by trial installations and customers with current maintenance. To license and use this service, add a Marshal IP Reputation Service entry in the list of Reputation Services.*

- *For more information about how to obtain the credentials required, see M86 Knowledge Base article Q12878.*

## ***Enabling a Reputation Service Rule***

The default email policy provided with MailMarshal SMTP includes a rule in the Connection Policies policy group that uses the SpamHaus Zen service in a Receiver rule.

### **To use the default Reputation Service rule:**

1. Ensure that SpamHaus Zen is included in the list of Reputation Services. This service is included by default in new installations.
2. In the left pane, expand the item **Email Policy** and select the policy group **Connection Policies**.
3. In the right pane, right-click the rule **Deny Spamhaus Blacklisted Senders at Receiver**. Choose **Enable** from the context menu.
4. To implement use of this rule, commit the configuration changes.

## PTR Lookups

MailMarshal SMTP can mark or refuse email from external servers that do not have correctly published Reverse DNS (PTR record) information. You can use this method to help guarantee the genuineness of a remote site, and as a layer of anti-spoofing protection.



**Notes:** Use PTR lookups with caution. Not all sites publish correct PTR information. Valid email traffic can be blocked by DNS checking if the sending site does not have PTR records, or if the records are faulty.

- If MailMarshal refuses a connection due to this policy, the connection is closed with the response: 554 no SMTP service here.

### To edit the PTR lookup policy:

1. In the Configurator, select **MailMarshal Properties** from the Tools menu.
2. Select **Host Validation** from the left pane.
3. To validate hosts sending incoming email using DNS information, select the check box **Validate connecting hosts in the DNS**.  
MailMarshal SMTP will perform a reverse DNS lookup on each IP address from which email is being sent.



4. Select an option using the radio buttons.
  - Choose **Accept unknown hosts** to accept email from hosts without appropriate DNS information, but log this fact to the MailMarshal SMTP Receiver text log.
  - Choose **Host must have a PTR record** to block messages from any host that does not have a valid DNS PTR record. Blocked messages are logged in the Windows Event Log and return the SMTP response: 554 No SMTP service here.
  - Choose **PTR Record must match the HELO connection string** to block messages from hosts whose PTR domain does not match the HELO identification sent by the server. This is the most restrictive option. Blocked messages are logged in the Windows Event Log and return the SMTP response: 554 No SMTP service here.
5. To implement the blocking, click **OK** or **Apply**.

## Blocked Hosts

You can maintain a list of servers that are never allowed to send any email through MailMarshal SMTP. MailMarshal SMTP will reject SMTP connections from these servers. Entries on this list will generally be servers outside your local LAN.

### To edit the list of Blocked Hosts:

1. In the Configurator, select **MailMarshal Properties** from the Tools menu.
2. Select **Blocked Hosts** from the left pane.
3. Add server names, IP addresses, or IP address ranges to the list. For information about the format of entries, see the Help.
4. To implement the blocking, click **OK** or **Apply** and then commit the configuration.

## Authentication by Account

MailMarshal SMTP can require each computer connecting to it to provide a user name and password. MailMarshal SMTP supports the CRAM-MD5, LOGIN, and PLAIN options for SMTP authentication. Additionally, authentication can be within a TLS session.

### To use authentication by account:

1. Create and maintain a list of accounts using the policy element Accounts. For more information see “Setting Up Accounts” on page 278.
2. Configure MailMarshal SMTP to advertise ESMTP authentication. For more information see “MailMarshal Properties - Advanced” on page 292.
3. Create a receiver rule using the condition “Where sender has authenticated”. For information about creating rules see “Understanding Rules” on page 129. For information about this rule condition see “Where sender has authenticated” on page 157.

## PREVENTING MALICIOUS EMAIL ATTACKS

MailMarshal SMTP helps to protect your network from intentional attempts to disrupt your operations. Denial of service attacks can cripple entire networks. Directory harvest attacks initially consume bandwidth and can result in your network receiving additional spam.

MailMarshal SMTP allows you to tailor denial of service prevention and directory harvest prevention features to suit your network and business requirements. Enable one or both forms of attack prevention if you believe that your network is vulnerable to attack.

## Understanding Denial of Service Attack Prevention

Denial of service (DoS) attacks cause target organizations to lose access to common business services, such as email. In an email DoS attack, the attacker floods email servers with messages or unused connections, causing the target email servers to slow down or cease operation.

### ***How MailMarshal SMTP Prevents Attacks***

MailMarshal SMTP prevents DoS attacks by the following means:

- Identifying external email servers that are attacking your network
- Blocking new connections from attacking servers for a period of time

MailMarshal SMTP determines that it is under attack when the number of new connections from any single external server in a short period exceeds a specified number. You specify both the period of time and the maximum number of allowable incoming messages.

### ***Optimizing DoS Attack Prevention Settings***

To determine the optimum settings for the DoS attack prevention parameters, you can log blocked hosts. Review the Senders Blocked by DoS Prevention report to see which servers were blocked. If you are affecting email flow from legitimate sources, you can change the settings to allow more messages through. You can also exclude specific hosts from DoS attack prevention by IP address or address range.

You configure DoS settings once for the entire MailMarshal SMTP array. However, MailMarshal SMTP applies the traffic limits you set at each email processing server. For example, if you use the default setting of 50 connections per minute and your installation is an array of five servers, your network can receive up to 250 connections per minute from any one external server (50 connections at each of 5 servers) When DoS prevention is triggered on one email processing server in a array, the other servers in the array are not affected.

When DoS prevention is blocking connections from a server, MailMarshal SMTP returns the SMTP response 421, Service not available. A legitimate server that receives this response will try again later.

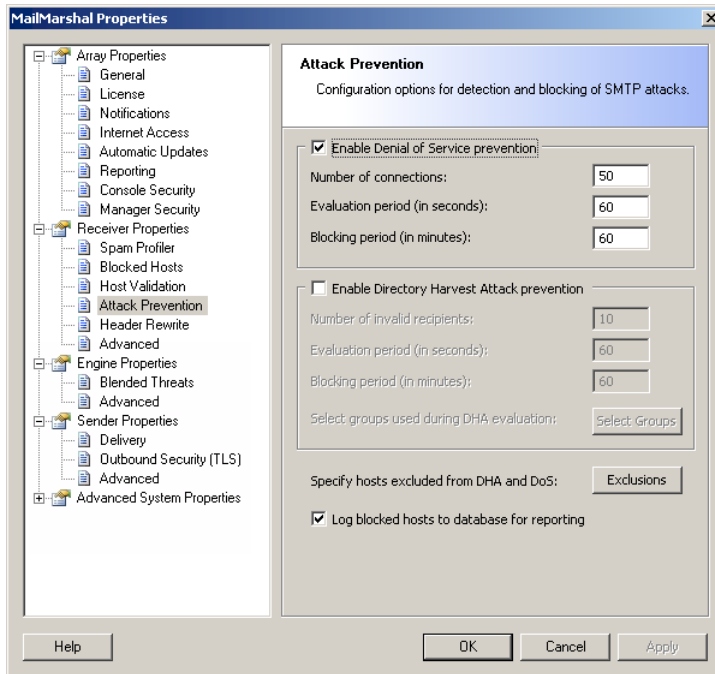
## Preventing Denial of Service Attacks

You configure DoS attack prevention by specifying the values MailMarshal SMTP will use to evaluate incoming email traffic, the blocking period, and any excluded hosts. You can adjust these values at any time.

### To configure DoS attack prevention:

1. In the Configurator, click **Tools** and select **MailMarshal Properties**.
2. Select **Attack Prevention** in the left pane.

3. Select **Enable Denial of Service prevention**, and specify values. For more information about the fields and settings, click **Help**.



4. Click **OK**.
5. Commit configuration to apply your changes.

## Enabling and Disabling DoS Attack Prevention

After configuring DoS attack prevention, you can enable or disable the feature without changing the configuration.

**To enable or disable DoS attack prevention:**

1. In the Configurator, click **Tools** and select **MailMarshal Properties**.
2. Select **Attack Prevention** in the left pane.
3. Select or clear **Enable Denial of Service prevention**, as needed.
4. Click **OK**.

## Understanding Directory Harvest Attack Prevention

In a directory harvest attack (DHA), an attacker attempts to identify valid email addresses by sending randomly-addressed messages to an email server. When a message reaches a recipient without being bounced back, the attacker enters the valid address in a database used for sending spam.

The attacker sends messages addressed either to random usernames, or to usernames that follow a common pattern, such as *firstname\_lastname@example.com*.

### ***How MailMarshal SMTP Prevents Attacks***

MailMarshal SMTP helps to prevent DHAs by the following means:

- Identifying external email servers that are attacking your network
- Blocking email from attacking servers for a specified period of time

DHA prevention identifies which email messages are addressed to valid users by comparing the recipient addresses to a list of users (email addresses). To ensure DHA prevention works correctly, you must configure MailMarshal to check one or more user groups that together contain all valid email addresses of all users in your environment.

DHA prevention checks each incoming email for a valid recipient. When the number of messages with invalid addresses, from a single server, and in a short period of time, exceeds a specified threshold, MailMarshal SMTP considers itself under attack and blocks incoming mail from the server. You determine the length of time to block the attacking server.

When DHA prevention terminates a connection, MailMarshal SMTP returns the SMTP response 556 Too many invalid recipient requests. While MailMarshal SMTP is blocking connections from a server, MailMarshal SMTP returns the SMTP response 421 Service not available. A legitimate server that receives this response will try again later. You can also exclude specific hosts from DHA prevention by IP address or address range.



**Note:** To ensure that DHA prevention works properly, enable it on a MailMarshal SMTP installation on the highest upstream email server in your network (closest to the public Internet).

## ***DHA Prevention Settings***

You configure DHA settings once for the entire MailMarshal SMTP array. However, MailMarshal SMTP applies the traffic limits you set at each email processing server. For example, if you use the default setting of 10 messages with invalid recipients per minute, and your installation is an array of five servers, your network can receive up to 50 invalid messages per minute from any one external server (10 messages at each of 5 servers)

When DHA prevention is triggered on one MailMarshal email processing server, other servers in the array are not affected. You can adjust the limits depending on your array and MX configuration.

To determine the optimum settings for the DHA prevention parameters, you can log blocked hosts. Review the Senders Blocked by DHA Prevention report to see which servers were blocked. If you are affecting email flow from legitimate sources, you can change the settings to allow more incorrectly addressed messages through. You can also exclude specific hosts from DHA attack prevention by IP address or address range.

## Preventing Directory Harvest Attacks

You configure DHA prevention by specifying the values MailMarshal SMTP will use to evaluate incoming email traffic. You can adjust these values until you determine the optimum settings for your network.

### To configure DHA prevention:

1. Create a list of all valid recipients by completing the following steps:
  - a. Create one or more Active Directory or LDAP user groups that together contain all the user email addresses in your environment. For more information, see “Creating and Populating User Groups” on page 179.

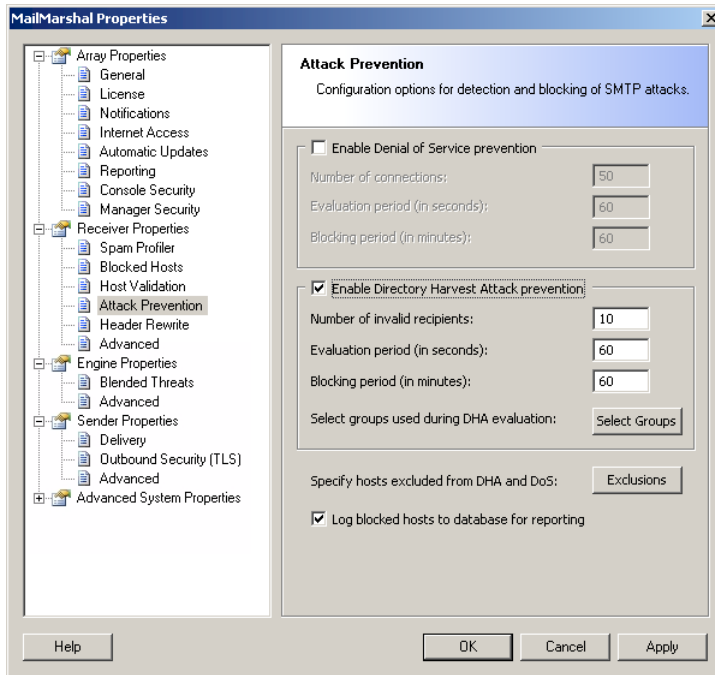


**Note:** Take care not to miss any users (email addresses) that are valid for email delivery. Select the group(s) at the highest point in the organizational hierarchy that you want to protect to ensure that you include all possible users in that hierarchy.

- b. Select these groups (or a group containing them) when configuring DHA prevention in the following steps.
2. In the Configurator, click **Tools** and select **MailMarshal Properties**.
3. Select **Attack Prevention** in the left pane.



4. Select **Enable Directory Harvest Attack prevention**, and specify appropriate values. Specify the group(s) you created to be used during evaluation. For more information about the fields and settings, click **Help**.



5. Click **OK**.
6. Commit configuration to apply your changes.

## Enabling and Disabling Directory Harvest Attack Prevention

After configuring DHA prevention, you can enable or disable the feature without changing the configuration. Use the following procedure:

**To enable or disable DHA prevention:**

1. In the Configurator, click **Tools** and select **MailMarshal Properties**.
2. Select **Attack Prevention** in the left pane.
3. Select or clear **Enable Directory Harvest Attack prevention**, as needed.
4. Click **OK**.

## FILTERING MESSAGES AND ATTACHMENTS

MailMarshal SMTP provides a framework that allows you to create an email policy in support of your Acceptable Use Policy.

A MailMarshal SMTP email policy is divided into policy groups. Each policy group consists of one or more rules.

For more information about the options available when creating policy groups and rules, see “Understanding Policy Groups” on page 127 and “Understanding Rules” on page 129.

The default email policy provided with MailMarshal SMTP contains several policy groups containing example and best practice rules:

**Connections and Policies**

Contains rules that block unwanted emails before they are downloaded to your network.

**Virus & Threats (Inbound)**

Contains rules that implement a recommended best practice for virus scanning of email messages sent to your environment from the Internet.

**Virus & Threats (Outbound)**

Contains rules that implement a recommended best practice for virus scanning of email messages sent from your environment out to the Internet.

**Attachment Management (Inbound)**

Contains rules that implement a recommended best practice for filtering attachments sent into your environment from the Internet.

**Attachment Management (Outbound)**

Contains rules that implement a recommended best practice for filtering attachments sent from your environment.

**Policy Management (Inbound)**

Contains rules to enforce your company policy in regards to receiving email containing prohibited language, credit card details, and so on. These rules also help you enforce SEC and SOC compliance.

**Policy Management (Outbound)**

Contains rules to enforce your company policy in regards to sending email containing prohibited language, credit card details, and so on. These rules also help you enforce SEC and SOC compliance.

**Spam**

Contains rules that implement a recommended best practice for detection and blocking of spam sent to your environment from the Internet.

**Automated Responses**

Contains rules that cause MailMarshal SMTP to send automated responses to various types of incoming email.

**Monitoring Only**

Contains rules that allow you to monitor selected content entering and leaving your environment. Some of these rules duplicate rules in the other policy groups. If you enable a monitoring rule, to avoid confusion you should disable any other rule that checks for the same conditions.

**Message Archiving**

Contains rules that specify how MailMarshal SMTP archives all inbound and outbound email.



---

## Chapter 6

# Understanding Email Policy, Policy Groups, and Rules

The MailMarshal SMTP **Email Policy** defines how MailMarshal SMTP treats each email message that it processes.

The Email Policy consists of one or more policy groups. Each policy group contains one or more rules. Each rule has three parts: User Matching, Conditions, and Actions.

When MailMarshal SMTP evaluates a message, it first checks the User Matching criteria for each policy group. If a message meets the User Matching criteria for a group, MailMarshal SMTP evaluates the message according to the User Matching and Conditions sections of each rule in the group. When a message meets the criteria of a rule, MailMarshal SMTP applies the specified actions to the message.

## UNDERSTANDING POLICY GROUPS

A **policy group** is a group of rules that share base User Matching conditions and a schedule of times when they apply. When MailMarshal SMTP is processing email, the conditions defined for a policy group must be met before any rule in that policy group is evaluated.

You can choose to use just a few policy groups, or many. For example, you could use one policy group to contain rules that apply to all messages outbound from the organization, and another policy group to contain rules that apply to all inbound messages. If your organization is divided into departments, you can also use policy groups to group rules governing email to and from each department.

Some default policy groups and rules are provided with MailMarshal SMTP. You should make changes and additions to meet your needs. M86 Security recommends a minimum of two policy groups: one for incoming email and one for outgoing email.

If you have more than one policy group, you can choose the order in which MailMarshal SMTP processes the groups.

You can set a schedule for a policy group. Any rules in the policy group will only be enabled at the scheduled times. You can choose to apply one or more of three different scheduling options:

- A repeating weekly schedule
- An absolute starting date and time
- An absolute ending date and time

**To create a policy group:**

1. In the left pane of the Configurator, select **Email Policy**.
2. Choose **New policy group** from the Action menu.
3. In the top pane on the Filtering Conditions window, select the User Matching conditions for this policy group.
4. The bottom pane of the Filtering Conditions window displays the conditions you have selected. If MailMarshal SMTP needs more information to define a condition, the description of the condition includes a hyperlink. Click the hyperlink to open a rule condition window that allows you to enter the required information.
5. On the Group Completion window, enter a name and optional schedule information for this policy group.

# UNDERSTANDING RULES

MailMarshal SMTP rules are divided into two types, receiver rules and standard rules. A policy group can contain rules of both types. Within a policy group, receiver rules will always be listed first, because they are always evaluated first for each message.

## Receiver Rules

MailMarshal SMTP applies receiver rules while the MailMarshal SMTP Receiver is receiving a message from a remote email server. A receiver rule can cause MailMarshal SMTP to refuse to accept a message based on the size or origin of the message. Because receiver rules are based on the limited information available while the message is being received, only a few conditions are available in these rules.

## Standard Rules

MailMarshal SMTP applies standard rules after a message has been fully received. They are processed by the MailMarshal SMTP Engine. Standard rules can evaluate a large number of conditions, because the complete email message is available for evaluation. Standard rules can also take a large number of quarantine and logging actions.

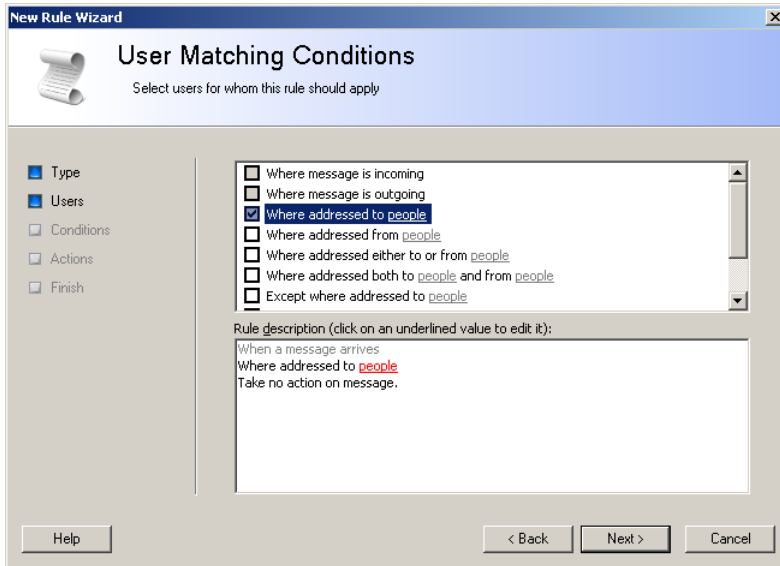
## Creating Rules

You can create as many rules as you need to implement your content security policy.

### To create a rule:

1. In the left pane of the Configurator, select a policy group.
2. Choose **New Rule** from the action menu.

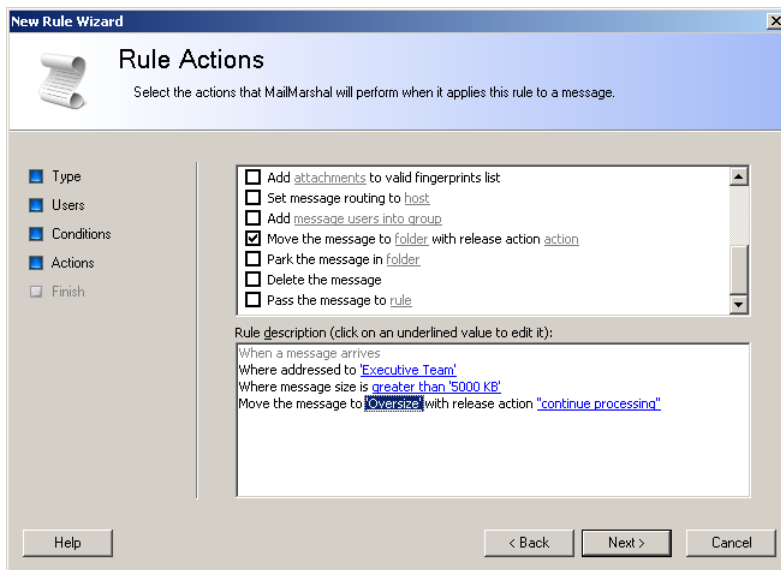
3. On the first window of the rule wizard, choose to create a receiver rule or a standard rule.
4. In the top pane on the User Matching window, select the User Matching conditions for this rule.



5. The bottom pane on the window displays the conditions you have selected. If MailMarshal SMTP needs more information to define a condition, the description of the condition includes a hyperlink. Click the hyperlink to open a window that allows you to enter the required information.
6. To continue to the Rule Conditions window, click **Next**.
7. In the top pane on the Rule Conditions window, select the conditions for this rule.
8. In the bottom pane on the window, review the conditions you have selected and specify any additional information required as for Step 5.



9. To continue to the Rule actions window, click **Next**.
10. In the top pane on the Rule Actions window, select the actions for this rule.
11. In the bottom pane on the window, review the actions you have selected and specify any additional information required as for Step 5.
12. On the Rule Completion window, enter a name and optional description for this policy rule. To create the rule and complete the wizard, click **Finish**.



## UNDERSTANDING USER MATCHING

MailMarshal SMTP performs user matching using the SMTP email addresses associated with a message. When you create policy groups and rules, you can include a number of User Matching conditions. User Matching conditions can refer to individual SMTP addresses, wildcard patterns of addresses, and user groups.

All the User Matching conditions in a policy group or rule must match (evaluate true) in order for MailMarshal SMTP to evaluate any other rule conditions.

The available User Matching conditions include the following:

**Where message is incoming**

Matches if the message is addressed to a domain that is included in the MailMarshal SMTP Local Domains list.

**Where message is outgoing**

Matches if the message is addressed to a domain that is not included in the MailMarshal SMTP Local Domains list.

**Where addressed to people**

Matches if a recipient of the message is found in the list of people specified.



**Note:** Whenever a condition requires a list of “people”, the list can contain individual email addresses, wildcard patterns to match sets of addresses such as domains, and MailMarshal SMTP user groups.

- For more information about wildcard characters, see Appendix A, “Wildcards and Regular Expressions.”
- For more information about which email addresses in a message MailMarshal SMTP checks, see M86 Security Knowledge Base article Q12238.

**Where addressed from people**

Matches if the sender of the message is found in the list of people specified.

**Where addressed either to or from people**

Matches if a recipient or sender of the message is found in the list of people specified.

**Where addressed both to and from people**

Requires two lists of people. Matches if the sender of the message is found in the first list of people specified, and the recipient of the message is found in the second list of people specified.

**Except where addressed to people**

Matches if **no** recipient of the message is found in the list of people specified.

**Except where addressed from people**

Matches if the sender of the message is **not** found in the list of people specified.

**Except where addressed either to or from people**

Matches if **no** recipient or sender of the message is found in the list of people specified.

**Except where addressed both to and from people**

Requires two lists of people. Matches if the sender of the message is **not** found in the first list of people specified, and **no** recipient of the message is found in the second list specified. “Except” matching criteria are the key to creating exception based policies. Rules that apply to all recipients with the exception of small specific groups help to ensure that security policies are uniformly applied. For instance, a rule might apply Where the message is incoming except where addressed to Managers.

## UNDERSTANDING RULE CONDITIONS

MailMarshal SMTP evaluates rule conditions within standard and receiver rules. MailMarshal SMTP checks rule conditions after any User Matching conditions. In general MailMarshal SMTP will only apply the rule actions to a message if all rule conditions evaluate true.

You can choose one or more rule conditions when you create or edit a rule in the Configurator. If the condition includes options, arguments, or variables, you can click a hyperlink in the rule wizard to open a window that allows you to specify values.

## Rule Conditions for Standard Rules

The following conditions are available for use in standard rules. They are further explained in the sections following:

- Where message is detected as spam by SpamEngine
- Where the result of a virus scan is
- Where the result of Blended Threat analysis is
- Where message attachment is of type
- Where attachment fingerprint is/is not known
- Where message size is
- Where the estimated bandwidth required to deliver this message is
- Where message contains attachment(s) named (file names)
- Where message triggers text censor script(s)
- Where the external command is triggered
- Where attachment parent is of type
- Where message attachment size is
- Where number of recipients is count
- Where message contains one or more headers (header match)
- Where number of attachments is count
- Where message is categorized as category
- Where message spoofing analysis is based on criteria
- Where the sender is/is not in the recipient's safe senders list
- Where the sender is/is not in the recipient's blocked senders list

- Where the attached image is/is not/may be inappropriate
- Where sender's IP address matches address



**Note:** *In a single rule, an AND relationship exists between multiple conditions. If a single rule includes multiple conditions, they must all evaluate true for the rule action to be taken. To match any of several conditions, place each one in its own rule. To create OR relationships between conditions, create a separate rule for each condition.*

## ***Where message is detected as spam by SpamEngine***

This condition allows you to take action on a message based on the result of evaluation by SpamProfiler, SpamBotCensor, and/or SpamCensor. You can use this condition in a rule that is processed early, to quarantine spam with minimal processing load. You can use this condition in combination with user group exclusions or other conditions to fine-tune recognition of spam.



**Note:** *You can also choose to reject messages at the Receiver based on SpamProfiler evaluation. For more information, see “Configuring SpamProfiler” on page 101.*

- *To use SpamBotCensor you must ensure that MailMarshal SMTP processing nodes are directly connected to the Internet (with no other gateway or firewall forwarding incoming messages to MailMarshal SMTP).*

On the rule condition window, select the anti-spam technologies you want to use. Choose to trigger the condition if all or any of the technologies classifies the message as spam. For more information, see Help.

## ***Where the result of a virus scan is***

This condition allows you to select from the virus scanning and cleaning features available in MailMarshal SMTP. Use the rule condition window to choose the desired virus scanning action and the results to be checked for.

The screenshot shows a dialog box titled "Rule Condition" with a close button (X) in the top right corner. The main title is "Where the result of a virus scan is" and the subtitle is "Specify the scanners MailMarshal will use and the scan results that trigger this rule condition." There are two radio buttons: "Scan with all scanners" (unselected) and "Scan with specific scanners:" (selected). Below the second radio button is a list box containing "McAfee for Marshal" (checked) and "Norman Virus Control" (unchecked). Underneath is the section "Where the result of the scan is:" with several checkboxes: "Contains Virus:" (checked), "and is Cleaned" (unchecked), "and Name Matches:" (unchecked, followed by an empty text box), "Password protected" (unchecked), "File is corrupt" (unchecked), "Virus scanner signatures out of date" (unchecked), "Could not fully unpack or analyze file" (unchecked), and "Unexpected scanner error" (unchecked). At the bottom are three buttons: "OK", "Cancel", and "Help".

You can choose the virus scanners MailMarshal SMTP uses when processing this condition.

- **All Scanners:** MailMarshal SMTP uses all configured virus scanners to scan all parts of the message and attachments. This option is the equivalent of virus scanning rules in MailMarshal SMTP 5.0 and earlier versions.
- **Specific scanners:** To limit the virus scan to specific installed scanners, choose this option then select the desired scanners from the list. MailMarshal SMTP uses the scanners you select. This setting can be useful if only some installed scanners support virus cleaning.

You can choose the scanner results that will cause this condition to trigger. To choose options, select the appropriate boxes on the Select Virus Scanner Results window.

- **Contains Virus:** The condition will trigger if any part of the message contains a virus. This is the basic condition.
- **...and is Cleaned:** When you select this item, the condition will only trigger if the code returned indicates that the virus was cleaned. This condition can be used in a Clean Viruses rule. You cannot choose this option if any non-DLL scanners are selected.

For further information about setting up virus cleaning rules, see the next section.

- **...and Name Matches:** When you select this item, the condition will only trigger if the name of the virus as returned by the scanner matches the text in the field. You can use this condition to modify the MailMarshal SMTP response based on certain virus behaviors. For instance you can choose not to send notifications to the sender address for viruses known to spoof the “from” address. You can use wildcard characters when you enter virus names. For more information, see “Wildcard Characters” on page 329 and “Regular Expressions” on page 331.
- **Password Protected:** When you select this item, the condition will trigger if the scanner reports the file as password protected.

- **File is corrupt:** When you select this item, the condition will trigger if the scanner reports the file as corrupt.
- **Virus scanner signatures out of date:** When you select this item, the condition will trigger if the scanner reports its signature files are out of date.
- **Could not fully unpack or analyze file:** When you select this item, the condition will trigger if the scanner reports that it could not unpack the file.
- **Unexpected scanner error:** When you select this item, the condition will trigger if the scanner reports an unknown error or the code returned is unknown.



**Note:** The detailed failure results depend on return codes provided by the individual scanner vendors.

With the exception of **Contains Virus** and **Unexpected scanner error**, the virus scanning features listed on the rule condition window can only be used with DLL based scanners. If you attempt to select options that are not supported by the scanners you have selected, MailMarshal SMTP will not allow you to save your selections.

Use the option “Unexpected scanner error” to specify an action MailMarshal SMTP should take when the code returned by the scanner is not known to MailMarshal SMTP. If this option is not selected in a rule condition, an unexpected return code will result in the message being dead lettered. For command line scanners, configure the list of return codes in the virus scanner properties. For more information about virus scanner properties, see “Using Virus Scanning” on page 212.

## **To Set Up Virus Cleaning**

If you want MailMarshal SMTP to attempt to “clean” viruses from email messages, you must install at least one DLL based virus scanner and set up two rules. The default configuration for new installations of MailMarshal SMTP includes appropriate rules.

The first rule must have these options selected:

- Contains Virus
- ...and is Cleaned



The second rule must be a standard virus blocking rule, using the option **Contains Virus** and invoking a move to a quarantine folder or other blocking action.

If a virus cannot be cleaned, MailMarshal SMTP takes the following actions:

1. MailMarshal SMTP applies the rest of the email policy.
2. If no quarantine (move to folder) or other blocking rule has been triggered after all rules have been applied, MailMarshal SMTP deadletters the affected message.
3. The message log and MailMarshal SMTP Engine log will indicate that the message still contains a virus.
4. If you choose to forward or process the affected message, MailMarshal SMTP displays a warning indicating that the message contains a virus.

### ***Where the result of Blended Threat analysis is***

This condition can be used to take action on messages that contain links or URLs recognized as dangerous by the MailMarshal SMTP Blended Threats Module (BTM) URL database.

If a message contains a URL that is not in the local copy of the database, the URL will be marked as unknown and submitted for analysis. You can choose to “hold” messages that contain unknown URLs and re-check them later when the database may have been updated. For more information, see “Hold the message” on page 167.



**Note:** *This option can improve security, but messages containing unknown URLs will be delayed.*

For details of the options available with this condition, see Help



**Notes:** *If the Blended Threats Module is not licensed, you will be warned when you save a rule that uses this condition.*

- *If the Blended Threats Module is not licensed, or the license expires while this condition is selected, URLs will not be checked by the Blended Threats Module. In this case the MailMarshal Engine log will show that the Blended Threats Module has not been used because it is not licensed.*
- *You can exclude trusted URL domains from BTM analysis. For more information, see “MailMarshal Properties - Advanced” on page 292.*
- *For more information about the Blended Threats Module, see M86 Knowledge Base article Q12876.*

## ***Where message attachment is of type***

MailMarshal SMTP checks the structure of all attached files to determine their type. MailMarshal SMTP can recognize over 175 types as of this writing.

The rule condition window provides a listing of file types organized by category. To select an entire category, select the check box associated with the category. To select individual types within a category, expand the category and select the check boxes associated with each type.



**Note:** *You can enter additional custom types by entering signature information in a configuration file. For information about the required procedures and structure of the file, see M86 Security Knowledge Base article Q10199.*

## ***Where attachment fingerprint is/is not known***

The “fingerprint” identifies a specific file (such as a particular image). The rule condition window allows you to choose to base the condition on fingerprints which are known or unknown.

To add a file to the list of “known” files, use the “add to valid fingerprints” rule action, or the “add fingerprints” option in the Console when releasing a message.

To delete a file from the list of “known” files, locate the file. It will be present on one or more of the MailMarshal SMTP email processing servers in the ValidFingerprints subfolder of the MailMarshal SMTP installation folder. Delete the file from this location on all servers then commit the MailMarshal SMTP configuration.



**Tip:** *The attachment fingerprint ability is intended to be used for a small number of images. If you add large numbers of files, MailMarshal SMTP performance will be affected.*

*This option can be useful to exclude certain images, such as corporate logos or signatures, from triggering quarantine rules. It is not intended as an anti-spam option.*

*For example to take action only on images that are not in the list of known images, use the following conditions:*

```
When a message arrives
Where message attachment is of type IMAGE
And where attachment fingerprint is not known
```

Files can also be “made known” by placing them in the ValidFingerprints subfolder of the Quarantine folder on any email processing server.

MailMarshal SMTP loads these fingerprints every 5 minutes, and when configuration is committed. For further information about this process, see M86 Security Knowledge Base article Q10543.

## ***Where message size is***

MailMarshal SMTP uses the size of the entire message, before unpacking, in this condition. The rule condition window allows you to choose a size and matching method (greater than a given size, less than a given size, between two sizes, not between two sizes, equal to or not equal to a size). If you choose to match between two sizes the matching is inclusive.



**Note:** *MailMarshal SMTP checks the size of the received message in its encoded format. This is typically 33% larger than the size reported by an email client.*

## ***Where the estimated bandwidth required to deliver this message is***

MailMarshal SMTP calculates the bandwidth required to deliver a message by multiplying the message size by the number of unique domains to which it is addressed. The rule condition window allows you to choose a total bandwidth and matching method (greater than a given size, less than a given size, between two sizes, not between two sizes, equal to or not equal to a size). If you choose to match “between” two sizes the matching is inclusive.

One use of this criterion is to move high-bandwidth messages to a “parking” folder for delivery outside peak hours. Another use is to reject high-bandwidth messages.

## ***Where message contains attachments named***

Use this condition to block files by extension, by specific file name, or by a wildcard pattern of the file name.

You can enter a list of file names in the rule condition window. When you enter information, you can use the wildcard characters asterisk (\*) and question mark (?). For example, the following are valid entries: \*. SHS; \*. VBS; \*. D0?

You can use this condition to quickly block dangerous file types such as VBS, or known virus attachments such as “creative.exe”. However, the condition checks only the file name and not the contents of the file. Use the condition “Where message attachment is of type” to check files by structure.

## ***Where message triggers text censor script(s)***

This condition checks textual content in some or all parts of the message and its attachments, depending on the settings defined in the specific script.

In the rule condition window, you can select a TextCensor script to be used in evaluating the message. You can add a script or edit an existing script. For detailed information about Scripts, see “Identifying Email Text Content Using TextCensor Scripts” on page 184.



**Note:** You can include more than one TextCensor script in this condition by selecting multiple boxes in the rule condition window. If you include more than one script, all included scripts must trigger for the rule to be triggered.

### ***Where the external command is triggered***

This option allows you to select one or more external commands MailMarshal SMTP uses to test the message. External commands can be executable programs or batch files. In the rule condition window, specify the commands. If more than one command is specified, all commands must be triggered for this condition to be triggered. For more information about external commands see “Extending Functionality Using External Commands” on page 225.

### ***Where attachment parent is of type***

This condition is intended to be used with the condition “Where message attachment is of type.” When this condition is selected, MailMarshal SMTP considers the file type of the immediate parent container as well as that of the attachment. For instance, you can check whether an image is contained in a MS Word document.

The rule condition window provides a listing of available parent types organized by category. To select an entire category, select the check box associated with the category. To select individual types within a category, expand the category and select the check boxes associated with each type. You can also choose to apply the condition to types in or out of the selected list. For instance, you can check that an image is not contained in a Word document.

*Tip: You can check for well known attachments, such as signature images in documents, using the condition “Where attachment fingerprint is/is not known.”*

### ***Where message attachment size is***

This condition checks the size of each attachment separately after all unpacking and decompression is complete. The size of an attachment can be greater than the size of the original message, due to decompression of archive files. The rule condition window allows you to choose a size and matching method (greater than a given size, less than a given size, between two sizes, not between two sizes, equal to or not equal to a size). If you choose to match “between” two sizes the matching is inclusive.

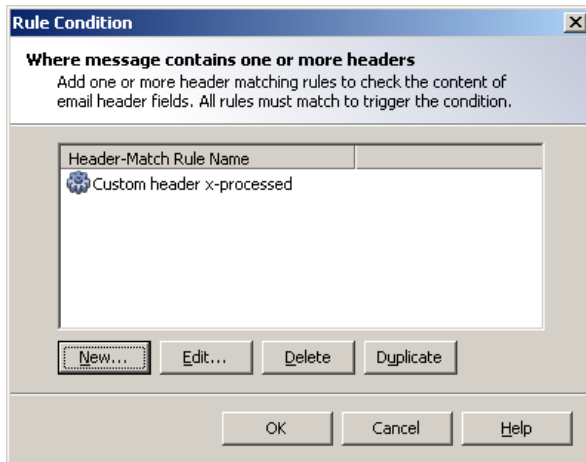
### ***Where number of recipients is count***

This condition checks the number of SMTP recipient addresses in a message. It is typically used to block messages with large recipient lists as suspected spam. The rule condition window allows you to choose a number and matching method (greater than a given number, less than a given number, between two numbers, not between two numbers, equal to or not equal to a number). If you choose to match “between” two numbers the matching is inclusive.

### ***Where message contains one or more headers***

This condition can be used to check for the presence, absence, or content of any message header, including custom headers. You can use this condition to check for blank or missing headers, or to reroute email.

Within the rule condition window, click **New** to create a new header match rule using the Header Matching Wizard. For more information about this Wizard, see “Using Rules to Find Headers” on page 219.



You can check more than one header match in a single condition. If you check more than one match, all matches must be true for the condition to be true (logical “and”). To match any of several header conditions (logical “or”), include more than one rule with one condition per rule.

To edit any Header Match condition (or view its details), highlight it, and then click **Edit** to restart the Header Matching Wizard. To delete a Header Match condition, highlight it, and then click **Delete**.



**Note:** You can only use Header Match conditions within the rule where you create them. To use the same condition in more than one rule, create it in each rule.

## ***Where number of attachments is count***

This condition is typically used to block messages with large numbers of attachments. The number of attachments can be counted using top level attachments only, or top level attachments to email messages including any attached messages, or all attachments at all levels.



**Note:** *“Top level attachments” are the files explicitly attached by name to an email message. Other files, such as the contents of a zip archive or images within a MS Word document, may be contained within the top-level attachments.*

The rule condition window allows you to choose a number and matching method (greater than a given number, less than a given number, between two numbers, not between two numbers, equal to or not equal to a number). If you choose to match “between” two numbers the matching is inclusive.

## ***Where message is categorized as category***

This condition allows action to be taken on messages that trigger a category script. Select one or more categories using the rule condition window.

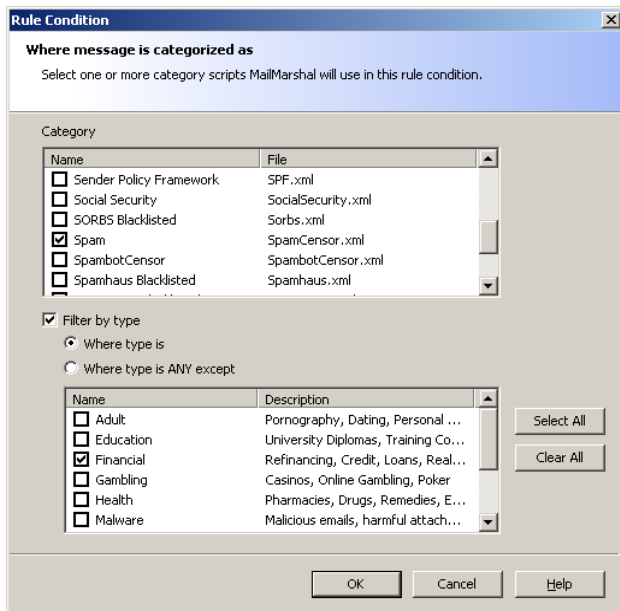
If a category includes multiple types (sub-categories), you can choose to include or exclude sub-types. To make a condition based on types, select (highlight) the parent item in the category list, check the associated box, select **Filter by type**, then select one or more items from the type list.



**Note:** *If **Filter by type** cannot be selected, no sub-categories are available for the category you have highlighted.*



You can also choose to exclude subtypes by clicking the option **Where type is ANY except**.



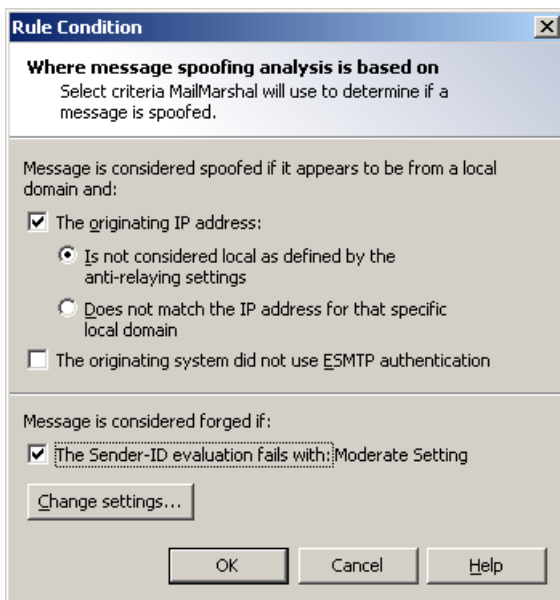
MailMarshal SMTP can automatically download updates to category scripts.

You can create and customize your own category scripts. Some example category scripts are provided with MailMarshal SMTP. For more information, see the white paper “MailMarshal SMTP for Anti-Spam,” available from the MailMarshal SMTP support page on the M86 Security website.

### ***Where message spoofing analysis is based on criteria***

This condition allows you to define when MailMarshal SMTP should consider a message to be spoofed. A **spoofed** message did not originate within the domain of the claimed sender email address. MailMarshal can check spoofing based on local domain servers, authenticated connections, and/or Sender ID.

In the rule condition window, select any of the detailed criteria for this condition.



MailMarshal SMTP evaluates the first two criteria, if selected, when the sender address (“From:” header or SMTP “Mail From:” address) of a message is within a Local Domain, as specified on the Local Domains window in the Configurator. These criteria do not apply for messages with From addresses in other domains.

**The originating IP address:**

Select this condition to check for spoofing based on the IP address of the computer which originated the message. Choose one of the following options to determine how MailMarshal SMTP checks the IP address:

**Is not considered local as defined by the anti-relaying settings:**

When you select this option, MailMarshal SMTP considers email with a local sender address “spoofed” if it does not originate from a computer allowed to relay. The list of computers allowed to relay is determined by the IP address ranges in the MailMarshal Relaying Table that is effective from this server.

This option is useful if you allow multiple servers and workstations in the local network to route email directly through MailMarshal SMTP.

**Does not match the IP address for that specific local domain:**

When you select this option, MailMarshal SMTP considers email with a local sender address “spoofed” if it is not delivered to MailMarshal SMTP from the correct Local Domain email server. The Local Domain server is the computer to which MailMarshal SMTP delivers messages for the specific SMTP domain of the “From:” address.



**Note:** *This is the more restrictive option. It requires all email originating within the organization to have been routed to MailMarshal SMTP from a trusted internal email server. Only messages accepted by the internal email server will be accepted by MailMarshal SMTP. This option can stop local users from “spoofing” addresses within the local domains.*

**The originating system did not use ESMTP authentication:**

Select this option to check for spoofing based on the login given by the system that delivered the message to MailMarshal SMTP. Use this condition (and not an IP address based condition) if you allow roving users to send email through MailMarshal SMTP using the Authentication feature. For more information about this feature see “Authentication by Account” on page 116.

MailMarshal evaluates the following criterion, if selected, for all messages.

**The Sender-ID evaluation fails:**

Select this option to evaluate the message using the Sender ID Framework. Click **Change Settings** to open a window that allows you to configure detailed Sender ID criteria.



**Note:** For more information about Sender ID, see M86 Security Knowledge Base article Q11559.

***Where the sender is/is not in the recipient’s safe senders list***

This condition allows you to take action on a message based on the list of “safe senders” maintained by a local message recipient through the Spam Quarantine Management Website. A typical use of this action is to create an exception to Spam rules, using the rule action “Pass the message to rule.” The default rules provided with new installations of MailMarshal SMTP include a rule to perform this function.

The user can enter an individual email address, or a wildcard pattern using the asterisk (\*) wildcard character.

In the rule condition window, choose whether to apply the condition if the sender is, or is not, in the recipient’s safe senders list.



**Note:** If the Safe Senders list is disabled (from the Administrator section of the SQM website), this condition has no effect.

## ***Where the sender is/is not in the recipient's blocked senders list***

This condition allows you to take action on a message based on the list of “blocked senders” maintained by a local message recipient through the Spam Quarantine Management Website. A typical use of this action is to create a rule that quarantines all email from addresses in the user’s blocked list. The default rules provided with new installations of MailMarshal SMTP include a rule to perform this function.

The user can enter an individual email address, or a wildcard pattern using the asterisk (\*) wildcard character.

In the rule condition window, choose whether to apply the condition if the sender is, or is not, in the recipient’s blocked senders list.



**Note:** *If the Blocked Senders list is disabled (from the Administrator section of the SQM website), this condition has no effect.*

## ***Where the attached image is/is not/may be inappropriate***

This condition allows you to take action on a message based on the result of analysis of attached images by Image Analyzer (an optional component licensed separately).



**Notes:** *You cannot select this rule condition if Image Analyzer is not licensed.*

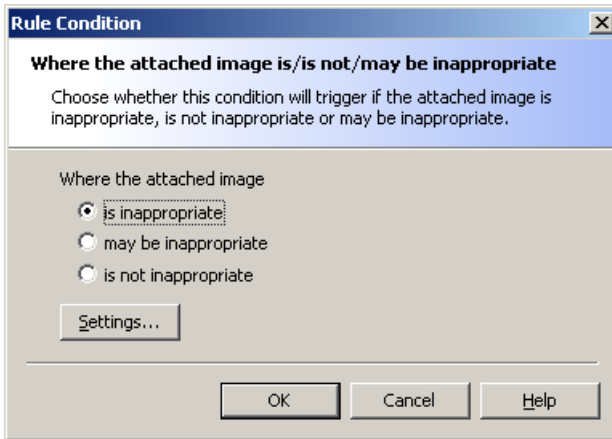
- *If the Image Analyzer license expires while this condition is selected, images will not be scanned by Image Analyzer. In this case the MailMarshal Engine log will show that Image Analyzer has not been used because it is not licensed.*

MailMarshal passes the following types of files that it unpacks from a message to Image Analyzer for analysis:

- Files MailMarshal recognizes as IMAGE types
- Binary files of unknown type.

Image Analyzer actually scans files of the following types: BMP, DIB, JPEG, JPG, JPE, J2K, JBG, JPC, PNG, PBM, PGM, PPM, SR, RAS, TIFF, TIF, GIF, TGA, WMF, PGX, PNM, RAS. For more information see M86 Security Knowledge Base article Q11622.

In the rule condition window, select the detailed criteria for this condition.



**The attached image is inappropriate:**

Specifies that the condition will trigger if Image Analyzer returned a score higher than the “inappropriate above” setting.

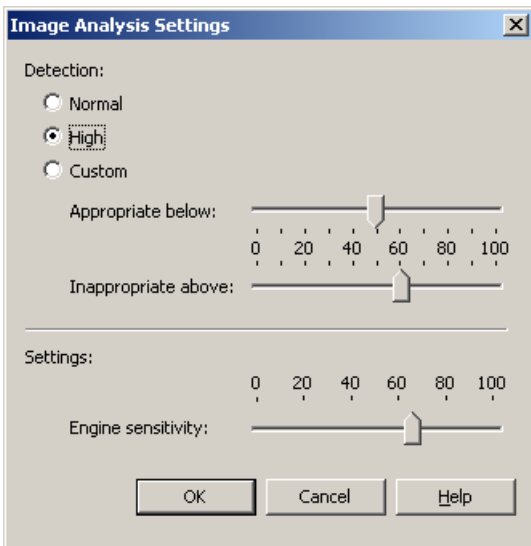
**The attached image may be inappropriate:**

Specifies that the condition will trigger if Image Analyzer returned a score between the “appropriate below” and the “inappropriate above” setting.

**The attached image is not inappropriate:**

Specifies that the condition will trigger if Image Analyzer returned a score below the “appropriate below” setting.

Click **Settings** to open the Image Analysis Settings window. This window allows you to configure advanced settings for Image Analyzer.



You can choose from the following basic detection settings:

**Normal:**

Specifies that the default Image Analyzer triggering levels should be used.

**High:**

Specifies that high sensitivity Image Analyzer triggering levels should be used. This setting detects more objectionable content, but also produces more false positive results.

**Custom:**

Allows you to set the Image Analyzer triggering levels using the slider controls, and to set advanced options using the control in the Settings section.

**Appropriate below:**

Specifies the maximum Image Analyzer return value that causes an image to be classified as “appropriate” (not likely to be pornographic). The default value is 49.

**Inappropriate above:**

Specifies the minimum Image Analyzer return value that causes an image to be classified as “inappropriate” (likely to be pornographic). The default value (Normal mode) is 75.

You can further tune Image Analyzer with one advanced option. The default setting has been selected after extensive testing.

**Engine sensitivity:**

Allows you to tune the sensitivity of the Image Analyzer engine. Reduce this value if a low false positive rate is more important than letting some offensive images through.

***Where sender's IP address matches address***

This condition can be used to take action on messages from one or more ranges of IP addresses.



**Note:** *This condition is also available in Receiver rules. To save resources and improve security, you should use this condition in a Receiver rule where possible.*

MailMarshal SMTP shows the configured ranges in the rule condition window. To add a range to the list, click **New** to open the Match IP Address window. To modify an existing address, highlight it, and then click **Edit**. To delete an existing address from the list, highlight it, and then click **Delete**.



Add or modify an address or range using the rule condition window. Select one of the three choices using the option buttons:

- **An IP Address:** Enter a single IP address in dotted quad format. For instance, enter “10.2.0.4”
- **A range of IP addresses:** Enter the starting and ending IP addresses for an inclusive range (two dotted quads). For instance, enter “10.2.1.4” and “10.2.1.37”
- **An entire network range:** Enter an IP address and a netmask in dotted quad format. For instance, enter “10.2.1.4” and “255.255.255.0” to match the entire 10.2.1.0 subnet.

The check box at the bottom of the window controls whether this address or range will be included or excluded from the condition match.

- To include the address or range, select the check box.
- To exclude the address or range, clear the check box.

## Rule Conditions for Receiver Rules

The following conditions are available for use in receiver rules.

- Where message is of a particular size
- Where sender's IP address matches address
- Where sender has authenticated
- Where sender's HELO name is/is not criteria
- Where sender's IP address is listed by Reputation Service
- Where the SPF evaluation result is

## ***Where message is of a particular size***

This condition is normally used with a “refuse message” action to refuse large messages. The rule condition window allows you to choose a size and matching method (greater than a given size, less than a given size, between two sizes, not between two sizes, equal to or not equal to a size). If you choose to match “between” two sizes the matching is inclusive.



**Note:** *The MailMarshal SMTP Receiver can only process this condition if the outside server has made an ESMTP connection and reported the message size. In order to check the size of all messages, you should repeat this condition in a standard rule to include messages received from sources that do not support ESMTP.*

## ***Where sender's IP address matches address***

This condition can be used to permit relaying, or to refuse messages, from one or more ranges of IP addresses. MailMarshal SMTP shows the configured ranges in the rule condition window. To add a range to the list, click **New** to open the Match IP Address window. To modify an existing address, highlight it, and then click **Edit**. To delete an existing address from the list, highlight it, and then click **Delete**.

Add or modify an address or range using the rule condition window. Select one of the three choices using the option buttons:

- **An IP Address:** Enter a single IP address in dotted quad format. For instance, enter “10.2.0.4”
- **A range of IP addresses:** Enter the starting and ending IP addresses for an inclusive range (two dotted quads). For instance, enter “10.2.1.4” and “10.2.1.37”
- **An entire network range:** Enter an IP address and a netmask in dotted quad format. For instance, enter “10.2.1.4” and “255.255.255.0” to match the entire 10.2.1.0 subnet.

The check box at the bottom of the window controls whether this address or range will be included or excluded from the condition match.

- To include the address or range, select the check box.
- To exclude the address or range, clear the check box.

### ***Where sender has authenticated***

This condition is normally used with the “Accept message” action to allow relaying by specific users. This condition will trigger if MailMarshal SMTP authenticated the remote system using an account and password. For more information about setting up accounts for authentication see “Setting Up Accounts” on page 278.

## ***Where sender's HELO name is/is not criteria***

This condition allows action to be taken based on the HELO name provided by the remote email server. Choose from the following options:

- **Where sender's HELO name is:** The condition will be true if the HELO name matches the criteria you select below.
- **Where sender's HELO name is not:** The condition will be true if the HELO name does not match the criteria you select below.
  - **A specific string:** Check this box and enter a character string to base the condition on an exact string (for example, AKLMAIL1)
  - **An IP address:** Check this box to base the condition on HELO strings that are IP addresses (not text names). Check the additional box "Correctly enclosed in brackets" to require brackets around the IP address.
  - **A fully qualified domain name:** Check this box to base the condition on HELO strings that are fully qualified domain names (FQDNs). For instance, AKLMAIL1.EXAMPLE.COM is a FQDN.



**Notes:** You can check one or more of the boxes.

- *Matching of a specific string supports wildcards. For more information, see "Wildcard Characters" on page 329.*

## ***Where sender's IP address is listed by Reputation Service***

This condition allows Reputation Service tests (DNS Blacklisting) to be applied. Choose the services to be used from the list in the Reputation Services window.

The window shows a list of all configured services. Select the check box for each service you want to use. Clear the check box for any service you do not want to use in this Condition. For information about how to configure reputation services, see “Reputation Services and DNS Blacklists” on page 112.

### ***Where the SPF evaluation result is***

This condition directs MailMarshal SMTP to check the message source using the Sender Policy Framework (SPF). Select the SPF results that trigger the condition using the option buttons.

To select a custom triggering value, and to configure advanced options, select **Custom** and then click **Change Settings**.

See Help for definitions of the options.



**Note:** For more information about SPF, see M86 Security Knowledge Base article Q11560.

## **UNDERSTANDING RULE ACTIONS**

MailMarshal SMTP rule actions are performed by standard and receiver rules. MailMarshal SMTP performs the actions if the user matching criteria and the other conditions of the rule evaluate true.

You can include more than one action in a MailMarshal SMTP rule. MailMarshal SMTP can also apply more than one set of actions to a message if more than one rule triggers. However, some actions are terminal actions. If a **terminal action** is performed, MailMarshal SMTP stops processing rules for the affected message.

## Rule Actions for Standard Rules

The following actions are available for selection in standard rules. Details of each action are given in the text following.

- Copy the message to folder with release action
- BCC a copy of the message
- Run the external command
- Send a notification message
- Strip attachment
- Write log message(s) with classifications
- Stamp message with message stamp
- Rewrite message headers
- Add attachments to valid fingerprints list
- Set message routing to host
- Add message users into group
- Move the message to folder with release action (*terminal action*)
- Park the message (*terminal action*)
- Hold the message (*terminal action*)
- Delete the message (*terminal action*)
- Pass the message to rule

### ***Copy the message***

This action copies the email message file to the specified quarantine folder. You can make the message processing log available in the same folder by selecting the check box at the bottom of the window. The message log showing how the message was processed will then be available in the Console.

You can specify how MailMarshal SMTP will process the message by default if it is released from this folder. Click the **Release action** link to specify the action. By default when a message is released, MailMarshal SMTP continues processing with the rule immediately after the rule that moved the message. For more information, see Help for the Release Action window.

When you select this action you can create a new folder. To create a folder, click **New Folder**. For more information see “Using Email Folders and Message Classifications” on page 212.

### ***BCC a copy of the message***

This action sends a blind copy of the message to one or more email addresses. Enter each address as a complete SMTP address (for example user@domain.topdomain). Separate multiple entries using semi-colons. You can also use variables in this field. The original message will not be modified in any way by this action, so the original recipient would not know a copy had been taken.

*Tip: You can use this action in combination with “delete the message” to effectively redirect a message to a different recipient.*

### ***Run the external command***

This action runs an external application. The application can be a Windows executable or batch file. For instance, an external command to release a message from quarantine is included with MailMarshal SMTP.

Choose one or more commands to be run from the list of pre-defined external commands. For information about defining external commands, see “Extending Functionality Using External Commands” on page 225. To run the same application with different parameters under different conditions, use more than one external command definition.

## ***Send a notification message***

This action sends one or more email messages based on the templates selected in the rule action window. To view or edit the details of a particular template, select it, and then click **Edit Template**. To create a new template, click **New Template**. The new template will automatically be selected for use when you return to the template selection window. For further information about templates, see “Notifying Users with Message Templates and Message Stamps” on page 194.

## ***Strip attachment***

This action removes one or more specific attachments from a message. Only the attachments that triggered the rule conditions for this rule will be stripped. This action would typically be used to remove attachments of specific file types or file names.



**Notes:** *MailMarshal SMTP does not save stripped attachments. If you use this action, normally you should copy the original message so that you can retrieve the attachment if necessary. You should stamp the message to inform the recipient that an attachment has been stripped.*

- *You can use this action in combination with a virus detection condition to strip infected attachments and allow the message to be delivered. To ensure that the message no longer contains a virus, you must include another virus scanning rule to run after the stripping action. Otherwise MailMarshal SMTP treats the message as possibly infected and will move it to the Dead Letter\Unpacking folder.*

## ***Write log message(s) with classifications***

This action writes a record classifying this message to the MailMarshal SMTP database.



Select one or more logging classifications from the list in the rule action window. Select the check box to write a logging classification for every component of the message (for example a separate record for each image file in a message). To view or edit the detailed information in the classification, click **Edit** in the selection window. To create a new classification, click **New** in the selection window. For details on classifications, see “Using Email Folders and Message Classifications” on page 212.

***Tip:** If a rule moves the message to a folder, MailMarshal SMTP automatically logs a classification for the message. In this case, usually you do not need to include a classification action as well.*

### ***Stamp message with text***

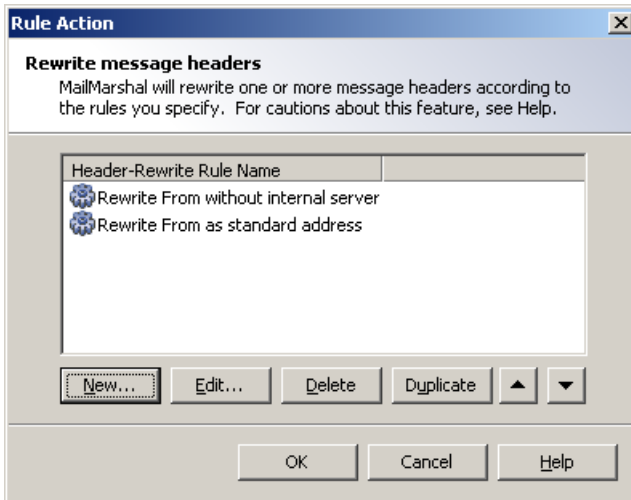
This action adds text to the top or bottom of the original message body.

In the rule action window, choose one or more message stamps to be used. A stamp will add text at the top or bottom of the message as selected when it is created. To view or edit the details of a particular message stamp, select it, and then click **Edit Stamp**. To create a new stamp, click **New Stamp**; the new message stamp will automatically be selected when you return to the stamp selection window. For details on message stamps, see “Notifying Users with Message Templates and Message Stamps” on page 194.

### ***Rewrite message headers***

Use this action to modify, add, or delete any message header, including custom headers. You can repair blank or missing headers, insert a notification into the subject, or reroute email.

Within the rule action window, click **New** to create a new header rewrite rule using the Header Rewrite Wizard. For more information about this Wizard see “Using Rules to Change Headers” on page 219.



You can include more than one Rewrite rule in the same action. If you include more than one Rewrite rule, the order of application of the rules can be significant. The rules listed first in the Header Rewrite window will be evaluated first. Adjust the order of evaluation by selecting a rule and using the up and down arrows on the window.



**Note:** Header Rewrite rules are only available within the rule where they are created. To perform the same action in more than one rule (or within a rule and the Header Rewrite function of the MailMarshal SMTP Receiver), create a Header Rewrite rule in each place.

## ***Add attachments to valid fingerprints list***

This action adds the attachments to the MailMarshal SMTP list of “valid fingerprints” (normally used for images or other files which require special treatment, such as company logos). In the rule action window, choose whether to add all attachments, or only images, to the list. For more information, see the rule condition “Where attachment fingerprint is/is not known.”

## ***Set message routing to host***

This action allows a message to be marked for sending to a selected email server. You can use this action to implement dynamic routing based on the recipient, the message headers, or the content of a message.

In the rule action window, enter a host name or IP address to which MailMarshal SMTP should send the message. Optionally enter a port number.

If you are integrating MailMarshal SMTP and MailMarshal Secure Email Server (for encryption and decryption processing), check the box *This is a MailMarshal Secure Email Server*.



**Note:** *If you are not directing mail to a MailMarshal Secure Email Server, ensure this box is **not** checked. For more information about this feature, see the MailMarshal Secure Email Server User Guide.*

MailMarshal SMTP uses this address when it attempts delivery, even if the message is “parked” first, or quarantined and later released. If several rules invoke this action, MailMarshal SMTP uses the last address.



**Notes:** *This action is not a terminal action. It sets the route for the message, but it does not send the message immediately or stop rule evaluation. MailMarshal SMTP continues to evaluate remaining applicable rules. Generally you should not use the actions **Delete the message** and **Set message routing to host** for the same message. If you do, the message will be deleted and not delivered.*

- *If a message is addressed to a MailMarshal SMTP POP3 domain, the message routing set by this action will not take effect.*

## ***Add message users into group***

This action allows you to add members to a MailMarshal SMTP user group based on any rule criteria, such as the sender or recipients of a message. You can use this action to automate the generation of lists of safe senders or blocked senders, based on other features of messages.



**Note:** *When you use this action to add members to a group, you should consider enabling automatic pruning to limit the size of the group. See “Pruning a MailMarshal SMTP Group” on page 182.*

In the rule action window, select one or more groups MailMarshal SMTP should add users to. Choose whether to add the sender or recipients.

You can create a new group by clicking **New Group**.

## ***Move the message***

This action moves the email message file to the specified quarantine folder. To make the message processing log available in the same folder, select the check box at the bottom of the rule action window. The message log explaining how the message was processed will then be available in the Console. If a new folder is required, click **New Folder** to start the New Folder Wizard.

You can specify how MailMarshal SMTP will process the message by default if it is released from this folder. Click the **Release action** link to specify the action. By default when a message is released, MailMarshal SMTP continues processing with the rule immediately after the rule that moved the message. For more information, see Help for the Release action window.

*This is a terminal action.* MailMarshal SMTP does not process any further rules for a message if this action is performed (unless the message is later released).

## ***Park the message***

This action moves the email message file to the specified parking folder for release according to the schedule associated with that folder. To create a new folder with a different schedule, click **New Folder** to start the New Folder Wizard.

*This is a terminal action.* If this action is performed, MailMarshal SMTP does not process any further rules for a message until the message is released from the parking folder. When a message is released from a parking folder, MailMarshal SMTP continues processing with the rule after the rule that parked the message.

## ***Hold the message***

This action moves the email message file to a special “hold queue” for the specific rule. You can configure a hold period after which the message will be re-submitted to the rule that caused the hold.

This action can be used with a Blended Threat Module “unknown” condition, to allow messages to be re-checked after the BTM database has been updated.

You can configure the number of times MailMarshal SMTP should retry the rule before continuing to the next rule. For details of the settings, see Help



**Warning:** Use this action only with a rule condition that can change when re-evaluated (such as the BTM unknown, BTM out of date, or scanner signature out of date conditions). If you use this action with a condition that never changes, affected messages will be delayed for no benefit.

*This is a terminal action.* If this action is performed, MailMarshal SMTP does not process any further rules for a message until the hold time expires. When a message is released from the hold queue, MailMarshal SMTP continues processing with the rule that caused the hold. If the number of retries is exceeded, MailMarshal SMTP continues processing with the rule after the hold rule.

You can force an immediate retry of held messages using the Hold Queues listing in the Console.

### ***Delete the message***

This action deletes the email message file. The message will not be sent to its original destination.

When you select this action, you can choose not to create an entry in the MailMarshal SQL logging database for the deleted message. By default MailMarshal logs information about deleted messages so that you can report on the reasons for deletions.

**Warning:** *If you choose not to create a SQL database entry, you will reduce database usage, but you will seriously affect your ability to audit MailMarshal activity. M86 Security recommends that you create SQL entries.*

*This is a terminal action.* MailMarshal SMTP does not process any further rules for a message if this action is performed.

### ***Pass the message to rule***

If no “terminal” rule action has been taken, this action allows a choice of which further rules to apply. Several choices are available in the rule action window:

- Skip the next rule (do not apply it).
- Skip to the next policy group (do not apply further rules in this policy group).
- Skip all remaining rules (pass the message through to the intended recipients).
- Skip to a specific policy group or rule.



**Note:** *It is only possible to skip to a rule which is evaluated after the current rule. The order of evaluation can be changed. See “Understanding the Order of Evaluation” on page 170.*

When skipping to a rule in a different policy group, remember that the parent policy group conditions can prevent its having any effect. For instance, skipping from the MailMarshal SMTP default Content Security (Inbound) policy group to the Content Security (Outbound) policy group is allowed, but rules in the Outbound policy group will have no effect on inbound messages.

## Rule Actions for Receiver Rules

The following actions are available for use in receiver rules.

- Accept message
- Refuse message and reply with message



**Note:** *These actions take effect immediately. If you use both types of actions in receiver rules, check the order of evaluation carefully to ensure that MailMarshal SMTP checks for any exceptions first.*

- Continue Processing Rules

### ***Accept message***

This action directs MailMarshal SMTP to accept the message for delivery subject to standard rules. The message could be relayed to an address outside the MailMarshal SMTP local domains. This condition can be used in conjunction with the condition “Where sender has authenticated” or an IP address match, to allow relaying by specific email users.

### ***Refuse message and reply with message***

This action directs MailMarshal SMTP to refuse the message. MailMarshal SMTP sends a SMTP response refusing delivery to the sending server. This action can be used in conjunction with a size-limiting condition to conserve bandwidth, or to refuse messages sent from specific problem addresses as detected by User Match, IP Address, or Reputation Service conditions.

On the rule action window, enter the SMTP response code and message to be returned as the message refusal.

- **Message Number:** Enter a SMTP message number (between 400 and 599) to return. The default number 550 is a standard SMTP “message refused” response.



**Note:** If you use a number in the 400 range the sending server will treat the refusal as temporary and will retry the delivery later. If you use a number in the 500 range the sending server will treat the refusal as permanent and will mark the message as undeliverable.

- **Message Description:** Enter a short message giving details of the reason for refusal. Within this message, the following variables are available:

Variable	Data inserted
{Recipient}	The “To:” SMTP address of the original message.
{Sender}	The SMTP address of the sender. This is the address in the “From” field unless it is empty, in which case the “Reply to” address is used.
{SenderIP}	The IP address of the sender.

### ***Continue Processing Rules***

This action has no effect on the message. It can be used with a logging-only condition such as “Where the SPF evaluation is set to log only.”

## **UNDERSTANDING THE ORDER OF EVALUATION**

The order in which MailMarshal SMTP evaluates policy groups and rules can affect the outcome of processing for a message. This is usually due to “terminal” actions that stop MailMarshal SMTP processing further rules for a given message.



For instance, by default MailMarshal SMTP evaluates virus scanning rules first. If a scanner reports a virus MailMarshal SMTP quarantines the message immediately. In this case MailMarshal SMTP does not perform any additional processing on the message.

MailMarshal SMTP evaluates policy groups and rules in “top down” order as it displays them in the Configurator.

## Adjusting the Order of Evaluation of Policy Groups

You can change the order of evaluation by changing the order of the policy group listing in the Configurator.

### To adjust the order of evaluation of policy groups:

1. Select **Policy Groups** in the left pane.
2. Select a policy group in the right pane.
3. Move the group up or down using the arrows in the toolbar or taskpad header.
4. Commit the MailMarshal SMTP configuration to effect the change in order.

## Adjusting the Order of Evaluation of Rules

You can change the order of evaluation by changing the order of the rule listing in the Configurator.

## To adjust the order of evaluation of rules:

### 1. Expand a policy group.

- To move a rule up or down within the policy group, use the arrows in the toolbar or taskpad header.
- To duplicate a rule, select it and then right-click and select **Duplicate**.
- To move or copy rules to another policy group, select one or more rules and then right-click and select **Copy To**.

### 2. Commit the MailMarshal SMTP configuration to effect the change in order.



**Notes:** *Within a policy group, MailMarshal SMTP lists all receiver rules first. MailMarshal SMTP processes receiver rules before it accepts the body of a message, so it always applies receiver rules before standard rules.*

- *If you have configured any rules with “Pass message to rule” or “Move/Copy to folder with release action”, MailMarshal SMTP checks for possible processing loops. To prevent problems, MailMarshal SMTP will disallow moving the rules, or disable some affected rules.*
- *You can move or copy a referring rule (a rule that includes one of the above actions).*
- *If you move or copy the referring rule to a policy group below the rule that is the target of the reference, MailMarshal SMTP disables the rule and raises a warning. Edit the rule to correct the action, and then re-enable it.*
- *You cannot move a target rule above a rule that refers to it.*
- *If you copy a target rule, the original rule remains in place and any copies are not targets, unless you copy the referring rule and the target in the same operation.*
- *You can select both a referring rule and target rule, and copy them to another policy group. MailMarshal updates the references in the copies, so that the new referring rule refers to the new target.*

## VIEWING EMAIL POLICY

You can list the entire email policy or a policy group in a format suitable for printing or copying to a file. For each rule, the listing shows the rule name, a verbose description, and a detailed listing of conditions and actions. The listing also indicates whether the rule is disabled.

### To print or copy a listing of the email policy or a policy group:

1. In the left pane of the Configurator, select **Email Policy** or a named policy group.
2. On the Action menu, choose **Print**.
3. MailMarshal SMTP presents the selected items in a print preview window.
4. To print the window contents, click the **Print** icon on the print preview window toolbar. You can also copy part or all of the window contents to the Clipboard using standard Windows commands.



---

## Chapter 7

# Understanding Email Policy Elements

Email policy elements are building blocks you can use when you create MailMarshal SMTP policy groups and rules. These elements help you to specify complex rule conditions and rule actions.

Some examples of each type of element are provided by default when MailMarshal SMTP is installed. These examples are used in the default email policy.

You can edit the existing elements or create new ones to support your policy requirements.

The following types of elements are available:

### **Connectors**

Allow you to import user and group information from Active Directory or LDAP servers, please see “Configuring Connectors” on page 177.

### **User Groups**

Allow you to apply policy based on email addresses. MailMarshal SMTP can retrieve groups from Active Directory or LDAP servers. You can also create local groups and enter members using wildcard characters.

MailMarshal SMTP uses two types of groups: MailMarshal SMTP groups and Imported groups. MailMarshal SMTP groups contain users and groups that you specify directly. Imported groups contain users and groups that you import from Microsoft Active Directory servers or LDAP servers, please see “Configuring User Groups” on page 179.

### **TextCensor Scripts**

Allow you to apply policy based on the textual content of email messages and attachments. You can create complex conditions using weighted combinations of Boolean and proximity searches, please see “Identifying Email Text Content Using TextCensor Scripts” on page 184.

### **Message Templates and Message Stamps**

Allow you to notify email users and administrators about MailMarshal SMTP actions, and insert disclaimers and confidentiality statements. You can include specific information about a message using variables, please see “Notifying Users with Message Templates and Message Stamps” on page 194.

### **Virus Scanners**

Allow you to check email messages for virus content. If a virus is found in a message you can attempt to clean it, please see “Using Virus Scanning” on page 212.

### **Email Folders and Message Classifications**

Allow you to quarantine or copy messages, or simply to record the results of MailMarshal SMTP evaluation. You can report on folder and classification actions using MailMarshal SMTP Reports, please see “Using Email Folders and Message Classifications” on page 212.

### **Email Header Matching and Rewriting**

Allow you to search for the content of email header fields using Regular Expressions. You can modify, add, or delete headers, please see “Header Matching and Rewriting” on page 218.

### **External Commands**

Allow you to extend MailMarshal SMTP functionality with customized conditions and actions, please see “Extending Functionality Using External Commands” on page 225.

### **Reputation Services**

Allow you to configure settings for externally maintained filtering lists that MailMarshal queries by DNS (also known as DNS Blacklists or DNS Blocklists), please see “Configuring Reputation Services” on page 228.

You can create or edit many policy elements on the fly while you are working with rules. For more information, see “Understanding Policy Groups” on page 127. You can also create elements in advance.

To work with policy elements, open the MailMarshal SMTP Configurator from the MailMarshal program folder. In the left pane of the Configurator select **Policy Elements**. To work with Connectors, in the left pane of the Configurator select **Connectors**.

## CONFIGURING CONNECTORS

Connectors allow MailMarshal SMTP to import user and group information from Active Directory and LDAP servers. Both Active Directory connectors and LDAP connectors import email addresses from user accounts, contacts, groups, and public folders. Additionally, LDAP connectors import names from other applications. For more information, contact M86 Security Technical Support.

For information about creating connectors, see “Creating Directory Connectors” on page 62.

### To edit a connector:

1. Select a connector in the right pane of the Configurator.
2. Click **Properties** on the taskpad header (Taskpad view) or the tools menu (Standard view).
3. On the General tab, you can edit the name and description of the connector.
4. On the Reload Schedule tab you can edit the schedule on which MailMarshal SMTP checks for updated information on the groups imported through this connector. You can choose to import once a day at a specific time, or more than once a day, or manually.

5. **If this is an Active Directory connector**, on the Active Directory Logon tab you can choose to connect as anonymous, or as a specific account. If you choose to connect using a specific account, enter the account details.
6. **If this is a LDAP connector**, edit the information provided.
  - a. On the LDAP Server tab you can edit the server name, port, and logon information. You can choose to connect as anonymous, or as a specific account. If you choose to connect using a specific account, enter the account details. You can enter or browse for a search root for this server. See the Help for full details of the fields on this tab. To change the attributes MailMarshal SMTP uses to retrieve group and member information from the LDAP server, click **Advanced**.
  - b. On the Group Attributes tab of the Advanced LDAP Properties window, edit the information MailMarshal SMTP will use to retrieve groups from the LDAP server. See the Help for full details of the fields on this tab.
  - c. On the User Attributes tab of the Advanced LDAP Properties window, edit the information MailMarshal SMTP will use to retrieve user email addresses from the LDAP server. See the Help for full details of the fields on this tab. For more information about how to retrieve all email addresses from a server, see M86 Security Knowledge Base article Q11877.
7. When you have completed all required changes to the connector, click **OK**.



# CONFIGURING USER GROUPS

You can use MailMarshal SMTP user groups within policy groups and rules. User groups allow you to apply policy to specific users. MailMarshal SMTP uses SMTP email addresses to perform user matching. You can create and populate user groups within MailMarshal SMTP by entering email addresses manually or copying them from other Groups. You can use wildcard characters when you define groups. You can also import user groups from an Active Directory environment or a LDAP server through a MailMarshal SMTP connector. MailMarshal SMTP updates the membership of imported groups automatically on a schedule you choose within the connector.

## Creating and Populating User Groups

Before you can import user groups, you must create MailMarshal SMTP connectors to provide access to the directory servers. For more information about creating connectors, see “Creating Directory Connectors” on page 62.

To create and maintain user groups, in the left pane of the Configurator, expand User Groups.

### To create a user group:

1. In the left pane of the Configurator, expand **User Groups**.
2. On the Action menu, choose **New User Group**.
3. Choose to create a MailMarshal SMTP group, or import groups through an Active Directory or LDAP connector.
4. **If you are importing a group**, select the Active Directory or LDAP connector you want to use. For more information about connectors, see “Configuring Connectors” on page 177. Click **Next**.
5. **If you are creating a MailMarshal SMTP group**, enter a name and description for the group.

6. **If you are importing a group**, enter the group name or click **Browse** to browse or search for available groups. You can select more than one group to import.



**Note:** *Best practice with imported user groups is to avoid using them directly in MailMarshal SMTP rules and policy groups. Configure the rules and groups using MailMarshal SMTP groups, and include the imported groups as members of the MailMarshal SMTP groups.*

7. When you have entered all the required information, click **Next**.

8. **If you are creating a MailMarshal SMTP group**, you can choose to edit the group immediately after creating it. To edit the group, on the final window of the New User Group wizard select **Edit the user group**.

9. To create or import the group, click **Finish**.

## ***Populating an Active Directory or LDAP Group***

Initially, an Active Directory or LDAP group will be empty of users. The group will be populated at the next scheduled update. You can use an imported group immediately in editing MailMarshal SMTP rules. However, you should not enable any rules that use a group until the group has been populated.

### **To populate an Active Directory or LDAP Directory group:**

1. Select the group in the left pane of the Configurator.
2. On the Action menu, select **Reload Group**.

## ***Adding Members to a MailMarshal SMTP Group***

You can add addresses or wildcard patterns to a MailMarshal SMTP user group.



**Note:** *You can also automatically harvest addresses from email messages into a group. For more information, see “Add message users into group” on page 166.*

**To add members to a MailMarshal SMTP user group:**

1. Select the appropriate user group from the right pane of the Configurator.
2. On the Action menu, select **Insert Users**.
3. In the New User Group window, enter an individual SMTP address, a partial address using wildcard characters, or a domain name.



**Note:** For more information about wildcard characters, see “Wildcard Characters” on page 329.

4. To add the value, click **Add** or use the Enter key.
5. The window remains open and you can enter additional values. If you entered an individual address, MailMarshal SMTP retains the domain name portion of the address in the field and you can simply enter another new user name.
6. When you have completed entry of all addresses, click **OK**.
7. Repeat this action to add other user groups.
8. When you have added all desired groups, click **OK**.

**Adding Groups to a MailMarshal SMTP Group**

You can add Active Directory, LDAP, and MailMarshal SMTP groups to a MailMarshal SMTP user group.

**To add other groups to a MailMarshal SMTP user group:**

1. Select a MailMarshal SMTP user group from the right pane of the Configurator.
2. On the Action menu, select **Insert Groups**.
3. In the Insert Into User Group window, select a group from the list.
4. To add the value, click **Add** or use the Enter key.

5. The window remains open and you can select additional values.
6. When you have completed your selection of groups, click **OK**.

### ***Pruning a MailMarshal SMTP Group***

You can configure MailMarshal SMTP to remove user addresses from a MailMarshal SMTP group. You can prune addresses that have not been seen for a time. You can also prune addresses if a group grows too large.

#### **To configure group pruning:**

1. Right-click a MailMarshal SMTP user group in the right pane of the Configurator, and select **Properties**.
2. On the Pruning tab, select one or both pruning options and set the limits.
3. Click **OK**.

For more information about pruning, see Help for the pruning tab, and see also M86 Security Knowledge Base article Q12772.

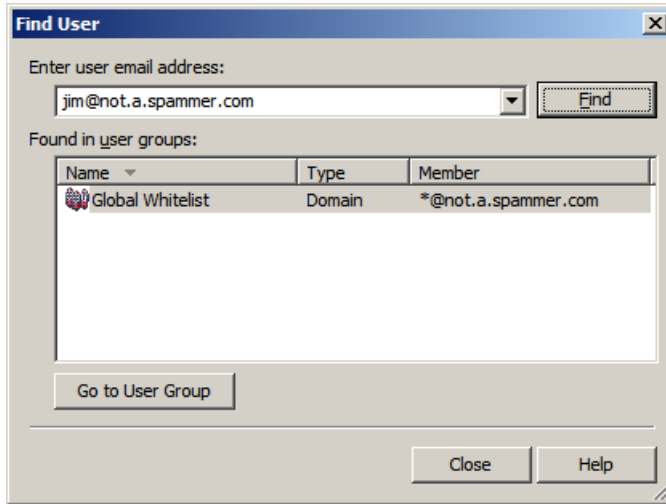
### ***Finding a User in Groups***

You can search all groups for a user (email address) or a wildcard pattern that matches an email address.

#### **To find a user:**

1. Select a user group or “All Groups” from the left pane of the Configurator.
2. On the Action menu, select **Find User**.

3. On the Find User window, enter a user name or a domain name and then click **Find**.
4. The result shows the group or groups that contain a matching entry.



## Moving and Copying Users and Groups

You can use drag-and-drop to move or copy a user name or an included user group from one parent group to another

To copy a user group, right-click it in the right pane of the Configurator. To make a copy, choose **Duplicate** from the context menu.

To add a user group to another user group, in the left pane select it and drag it over the target group in the same pane.

To move a user to another user group, in the left pane select it and drag it over the target group in the same pane. To copy the user to the group, hold down **Ctrl** while dragging the user.

To copy or move users, select a user group in the left pane to view its members in the right pane. To move group members, select one or more members in the right pane and drag them over a group in the left pane. To copy group members, hold down the Ctrl key while dragging.

## IDENTIFYING EMAIL TEXT CONTENT USING TEXTCENSOR SCRIPTS

**TextCensor scripts** check for the presence of particular lexical (text) content in an email message. MailMarshal SMTP can check one or more parts of a message, including the message headers, message body, and any attachments that can be lexically scanned. Apply TextCensor scripts to email messages by using standard rules.

A script can include many conditions. Each condition is based on words or phrases combined using Boolean and proximity operators. The script matches, or triggers, if the weighted result of all conditions reaches the target value you set.



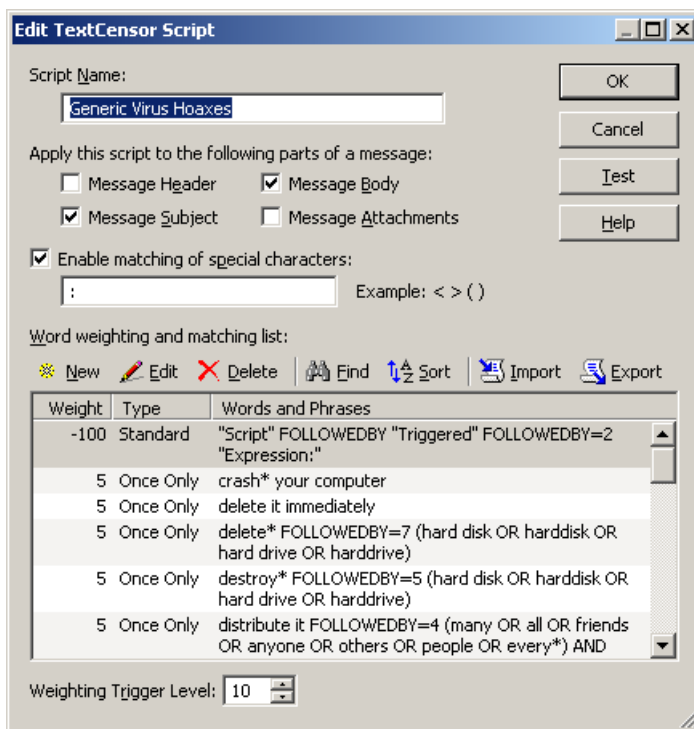
**Note:** For MailMarshal to detect and block explicit language (such as profanity and pornographic language), objects such as the Email Policy rules and the TextCensor scripts need to contain that explicit language. Anyone who has permission to use the MailMarshal Configurator, Console, or Reports may be exposed to this explicit language. As this language may be objectionable, please follow your company's policy with respect to exposure to content of this type.

## Creating Scripts

To work with TextCensor Scripts, select TextCensor Scripts in the left pane of the Configurator.

### To add a TextCensor Script:

1. In the left pane of the Configurator, expand **TextCensor Scripts**.
2. On the Action menu, choose **New TextCensor Script** to open the TextCensor Script window.



3. Enter a name for the script.

4. Select which portions of an email message you want this script to scan by selecting one or more of the check boxes Subject, Headers, Body, and Attachments.



**Note:** The script will check each part separately.

For instance, if you select both Headers and Message Body, the script will be evaluated once for the headers, then again for the body. Script scoring is not cumulative over the parts.

5. By default you can only use alphanumeric characters A-Z and 0-9 in TextCensor items. If you need to match any non-alphanumeric characters, select the check box **enable matching for special characters**, then enter any special characters to be matched in the field. For instance, to match the HTML tag fragment <scri pt you must enter the < in this field. To match parentheses ( ) you must enter them in this field.



**Note:** The equal sign = is an exception. To match this character in a TextCensor item, simply enclose it within double quotes: " = " .

6. Add one or more TextCensor items. To begin adding items, in the TextCensor Script window click **New** to open the TextCensor Item window.

7. Select a weighting level and type for the item. For more information, see “Script and Item Weighting” on page 188.



8. Enter the item text, optionally using Boolean and proximity operators. For example you could enter

(Dog FOLLOWEDBY hous\*) AND NOT cat

In this example the item weighting will be added to the script total if the scanned text contains the words “dog house” (or “dog houses”, and so on) in order, and does not contain the word “cat”.



**Note:** *TextCensor items are case insensitive by default. However, quoted content is case sensitive. For example “textcensor” would not trigger on the first word in the body of this note.*

9. To add the value to this script, click **Add** or use the Enter key. The New TextCensor Item window will remain open and you can create additional items.
10. When you have entered all items, click **Close** to return to the New TextCensor Script window.
11. Select a Weighting Trigger Level. If the total score of the script reaches or exceeds this level, the script will be triggered. The total score is determined by evaluation of the individual lines of the script.
12. To set the order of evaluation, click **Sort List**. Sorting sets items with negative weighting levels to evaluate first.



**Note:** *Because evaluation of a script stops when the trigger level is first reached, setting evaluation order is important.*

## Editing Scripts

You can change the content of an existing script, including the individual items and overall properties.

**To edit a TextCensor Script:**

1. Double-click the script to be edited in the right pane.
2. Edit an item by double-clicking it.
3. Delete an item by selecting it, and then clicking **Delete**.
4. Change the contents of any fields such as the script name, parts of the message tested, special characters, and weighting trigger level.
5. Use the **Sort List** button to adjust the order of items.
6. Click **OK** to accept changes or **Cancel** to revert to the stored script.

## Duplicating Scripts

Duplicate a script if you want to use it as the basis for an additional script.

**To duplicate a TextCensor Script:**

1. Right-click the script name in the Configurator.
2. Choose **Duplicate** from the context menu.
3. After duplicating the script, make changes to the copy.

## Script and Item Weighting

Each script has a trigger level expressed as a number. If the total score of the content being checked reaches or exceeds this level, the script is triggered. The total score is determined by summing the scores resulting from evaluation of the individual items in the script.

Each line in a script has a positive or negative weighting level and a weighting type. The type determines how the weighting level of the line is figured into the total score of the script.

There are four weighting types:

Weighting Type	Description	Details
Standard	Each match of the words or phrases will add the weighting value to the total.	If the weighting level of this item is 5, every match will add 5 to the total.
Decreasing	Each match of the words or phrases will add a decreasing (logarithmic) weighting value to the total. Each additional match is less significant than the one before.	If the weighting level of this item is 5, the first five matches will add 5, 4, 4, 3, and 3 to the total.
Increasing	Each match of the words or phrases will add an increasing (exponential) weighting value to the total. Each additional match is more significant than the one before.	If the weighting level of this item is 5, the first five matches will add 5, 5, 6, 6, and 7 to the total.
Once Only	Only the first match of the words or phrases will add the weighting value to the total.	If the weighting level of this item is 5, this item will contribute at most 5 to the total, no matter how many times it matches.

You can use negative weighting levels and trigger levels to allow for the number of times a word may appear in an inoffensive message. For instance, if “breast” is given a positive weighting in an “offensive words” script, “cancer” could be assigned a negative weighting (since the presence of this word suggests the use of “breast” is medical/descriptive).



**Note:** Because MailMarshal SMTP stops evaluation of a script when it reaches the trigger level, you should make sure that items with negative weighting are set to evaluate first. Use the **Sort List** button to set the order of evaluation correctly.

## Item Syntax

A TextCensor script contains one or more items, each consisting of words or phrases and Boolean or proximity operators.

- You can use the asterisk (\*) wildcard at the end of a word only (for example “be\*” matches “being” and “behave”).
- You can use parentheses to set the order of evaluation and for grouping. You can also use parentheses to help readability in complex lines.
- You can use Boolean and proximity operators. Enter the operators in capital letters.
- When you use NEAR or FOLLOWEDBY, a **word** is defined as any group of one or more contiguous alphanumeric characters, bounded at each end by non-alphanumeric characters. If any non-alphanumeric characters have been included as “special characters”, each single special character is also counted as a word.

***Tip:** For instance, by default S-P-A-M counts as four words. If the “-” character is entered as a “special character,” then the same text counts as 7 words.*

The Boolean operators TextCensor supports are shown in the following table.

Operator	Function	Example
AND	Matches when all terms are present	Dog AND cat
OR	Matches when any term is present	dog OR cat dog OR (cat AND rat)
NOT	Logical negation of terms; use after other operators; means “anything else but.”	Dog AND NOT cat Dog FOLLOWEDBY (NOT house)

Operator	Function	Example
NEAR	Matches when two terms are found within the specified number of words of each other. The default is 5.	Dog NEAR=2 bone
FOLLOWEDBY	Matches when one term follows another within the specified number of words. The default is 5.	Dog FOLLOWEDBY=2 house
INSTANCES	Matches when a term is found the specified number of times. You must specify a value.	Dog INSTANCES=3

MailMarshal SMTP allows the INSTANCES operator for compatibility with earlier TextCensor scripts, but it is deprecated. You can use item weighting types to produce the same result with improved performance.

## Importing Scripts

You can import scripts in files. Use this function to copy a script from another MailMarshal SMTP installation, or to restore a backup

### To import a TextCensor Script from a CSV or XML file:

1. On the Action menu, choose **New TextCensor Script** to open the TextCensor Script window.
2. Click **Import**.
3. Choose the file to import from, and click **Open**.
4. In the Edit TextCensor Script window, click **OK**.



**Note:** *TextCensor Scripts exported from MailMarshal SMTP 4.2.5 and earlier versions do not include the Weighting Trigger Level, Special Characters, and Apply to following parts settings. If you are importing such a script, you must add this information by editing the script after you import it.*

## Exporting Scripts

You can save scripts in files. Use this function to move a script between MailMarshal SMTP installations, or to edit a script in another application such as Microsoft Excel.

### To export a TextCensor Script to a CSV or XML file:

1. Double-click the name of the script to be exported in the right pane to open the Edit TextCensor Script window.
2. Click **Export**.
3. Enter the name of the file to export to, and click **Save**.
4. In the Edit TextCensor Script window, click **OK**.

## TextCensor Best Practices

To use TextCensor scripts effectively, you should understand how the Text Censor facility works and what it does.

MailMarshal SMTP applies TextCensor scripts to text portions of messages. Depending on the portions you select, a script can apply to headers, message bodies, and attachment content. MailMarshal SMTP can generally apply TextCensor scripts to the text of Microsoft Office documents and Adobe PDF files, as well as to attached email messages and plain text files.

### *Constructing TextCensor Scripts*

The key to creating good TextCensor scripts is to enter exact words and phrases that are not ambiguous. They must match the content to be blocked. Also, if certain words and phrases are more important, you should give those words and phrases a higher weighting. For instance, if your organizational Acceptable Use Policy lists specific terms that are unacceptable, you should give those terms a higher weighting to reflect the policy.

In creating TextCensor scripts, strike a balance between over-generality and over-specificity. For instance, suppose you are writing a script to check for sports-related messages. If you enter the words “score” and “college” alone your script will be ineffective because those words could appear in many messages. The script will probably trigger too often, potentially blocking general email content.

You could write a better script using the phrases “extreme sports”, “college sports” and “sports scores” as these phrases are sport specific. However, using only a few very specific terms can result in a script that does not trigger often enough.

You can strike a good balance using both very specific and more general terms. Again using the example of sports related content, you could give a low positive weighting to a phrase such as “college sports.” Within the same script you could give a higher weighting to the initials NBA and NFL, which are very sports specific.

## ***Decreasing Unwanted Triggering***

TextCensor scripts sometimes trigger on message content which is not obviously related to the content types they are intended to match.

### **To troubleshoot unwanted triggering:**

1. Use the problem script in a rule which copies messages and their processing logs to a folder. You could call this folder “suspected sports messages”.
2. After using this rule for some time, check on the messages that have triggered the script. Review the message logs to determine exactly which words caused the script to trigger. See “Viewing Messages” on page 238.

3. Revise the script by changing the weighting, weighting type, or key words, so as to trigger only on the intended messages.
4. When you are satisfied, modify the rule so as to block messages that trigger the script. You could also choose to notify the sender and/or the intended recipient.

## Testing Scripts

When you are working with a TextCensor script in the Configurator, you can test it against a file or pasted text.

### To test a TextCensor Script:

1. On the New or Edit TextCensor Script window, click **Test**.
2. **To test using a file**, select **Test script against file**. Enter the name of a file containing the test text (or browse using the button provided).
3. **To test using pasted text**, select **Test script against text**. Type or paste the text to be tested in the field.
4. Click **Test**. MailMarshal SMTP will show the result of the test, including details of the items which triggered and their weights, in the **Test Results** pane.

## NOTIFYING USERS WITH MESSAGE TEMPLATES AND MESSAGE STAMPS

MailMarshal SMTP provides two ways of sending notifications by email.

**Message stamps** are short blocks of text that can be added to an email message. You can use a stamp to add a company disclaimer, or to warn the recipient of a message that MailMarshal SMTP has modified it.



**Message templates** are complete email messages that can be sent to a user or administrator. MailMarshal SMTP uses templates for system notifications such as non-delivery reports. You can also use them to provide auto-responders or other custom notices. MailMarshal SMTP can use special digest templates to provide users with summary information about quarantined email.

MailMarshal SMTP applies message stamps to both HTML and plain text portions of an email message. Message templates can also include plain text and HTML bodies.

Variables can be used in both templates and stamps. **Variables** are specially formatted strings you can insert in a stamp or template. When MailMarshal SMTP uses the stamp or template, it replaces the variables with information about the specific message. This facility allows you to provide detailed information about the actions MailMarshal SMTP has taken on a specific message.

## Message Templates

Message templates are used when MailMarshal SMTP sends a notification email message based on the outcome of rule processing. The most common use of notification messages is to notify appropriate parties when an email message is blocked.

Notifications are a very powerful tool to inform and modify user behavior. When well thought out and constructed, they can save the administrator a lot of time.

You can also use a notification to set up a general auto responder based on message headers or content. For instance, MailMarshal SMTP could respond to a message to `robot@ourcompany.com` with the subject "Send Catalog" by returning the product catalog to the sender as an email attachment.

The same rule can send several notification messages. For instance, if MailMarshal SMTP detects a virus you could choose to send different messages to an email administrator, the external sender, and the intended internal recipient of the message.

You can attach files to a notification. Attachments can include the original message, the MailMarshal SMTP processing log for the message, and any other file (such as a virus scanner log file).

You can create a template as plain text, HTML, or both. If you choose to create a template with both HTML and plain text bodies, you must edit the two bodies separately. If you choose to create a template with HTML only, MailMarshal SMTP will automatically generate a plain text equivalent of the template with similar formatting.

You can include links to images in HTML templates. You cannot embed images.



**Note:** In addition to rule notification templates, MailMarshal SMTP uses a number of pre-configured templates for administrative notifications (such as delivery failure notifications). For more information about modifying these templates, see “MailMarshal Properties - Advanced” on page 292.

## Creating a Message Template

To work with templates, select Message Templates in the left pane of the Configurator.

### To create a message template:

1. In the left pane of the Configurator, select **Message Templates**.
2. On the Action menu, select **New Message Template** to open the Message Template window.

3. By default, MailMarshal SMTP creates a HTML message body. MailMarshal SMTP will automatically generate a plain text equivalent of the message body when using the template. To choose a plain text body or edit both types separately, click **Options**.
4. To see additional address fields, click **Options**.
5. Enter a name for the template.
6. Enter appropriate information in the Header Details section. For instance, enter the email address to which replies should be sent in the **Return Path** field.

***Tip:** The MailMarshal SMTP default configuration includes numerous templates. These are a good source of ideas for the creation of new templates.*

7. Enter text in the body section. To view the raw HTML, right-click in the HTML pane and select **Edit Raw HTML**. Edit the HTML, or paste HTML source from another editor, then click **OK** to return to the message template window.
8. You can attach files to the notification, including the original message, the MailMarshal SMTP message processing log, and other files. To attach one or more files, select the appropriate box(es) and enter the file names if necessary.
9. You can use variables marked with braces { }. To see a list of variables available in any field, type { to open a context menu. You can also enter variable names manually. You can use nested variables. For details of the variables available in templates, see “Using Variables” on page 204.



**Note:** When sending a notification to the original sender of an email message, use the {ReturnPath} variable in the To: field to reduce the chance of looped messages. Do not use the {ReturnPath} variable in the From: field.

## Creating Digest Templates

The MailMarshal SMTP Array Manager uses digest templates to deliver periodic message digests to users who self-manage end-user management folders. For details of digesting, see “Setting Up Message Digests” on page 308.

Digest templates are similar to message templates. The key differences are:

- You cannot attach files to digest templates.
- You must associate each digest template with a message digest. See “Setting Up Message Digests” on page 308.

Digest templates support variables specific to the digesting function that are not available in message templates. These variables allow MailMarshal SMTP to provide a list of information about several messages within the same notification message. The most important of these variables is the HTML digest table variable `$MessageDigestTableHTML`.

The following arguments are available to customize the behavior of this variable. All arguments are optional.

Detail Level	Results
BRIEF	Single line for each message, with From, Subject, Date, and small portion of message body (default level).
COMPACT	Two lines for each message; portion of message body starts on second line.
VERBOSE	Longer version including up to 200 characters of message body.

Option	Results
RELEASE	Show the message release link for each message (default option).

Option	Results
NORELEASE	Do not show the message release links.
RELEASEURL= <i>url</i>	Specify the URL path to the Release webpage used for this digest (see example below). Defaults to the URL of the local MailMarshal Spam Quarantine Management website. A URL could be specified, for instance, in the digests for user groups that cannot browse to the default location.
GROUP	Group entries by folder, for digests covering multiple folders.
SHOWFROM= <i>yes/no</i>	Show the sender address. Defaults to yes.
SHOWTO= <i>yes/no</i>	Show the recipient address. This option will generally be required when digests for multiple users are sent to the same address. Defaults to no.

**Example:**

```
{ $MessageDigestTableHTML=COMPACT, GROUP, SHOWFROM=no,
RELEASEURL=http://extranet.example.com/SpamConsole}
```

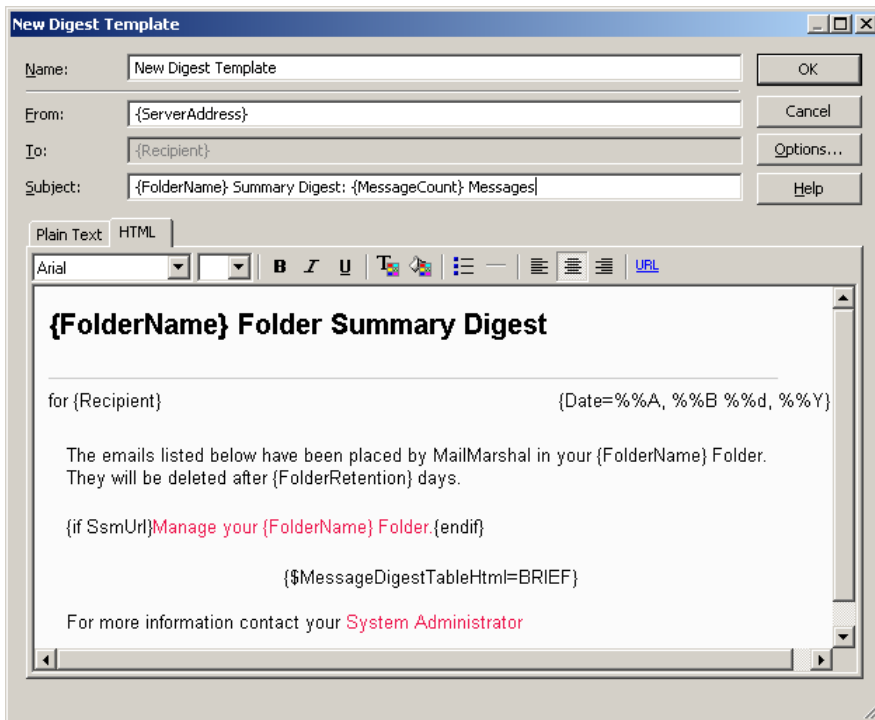
For details of other variables available in digest templates, see “Using Variables” on page 204.



**Note:** To obtain the best results with digest templates, edit the plain text and HTML versions of the template separately using the “Both” option.

## To create a digest template:

1. In the left pane of the Configurator, select **Message Templates**.
2. On the Action menu, select **New Digest Template** to open the Digest Template window.



3. By default, MailMarshal SMTP populates the template with basic information. MailMarshal SMTP creates separate HTML and plain text message bodies. To choose to use only one of the two types, click **Options**.
4. To see additional address fields, click **Options**.
5. Enter a name for the template.

6. Enter appropriate information in the Header Details section. For instance, enter the email address to which replies should be sent in the **Return Path** field.
7. Enter text in the body section. To view the raw HTML, right-click in the HTML pane and select **Edit Raw HTML**. Edit the HTML, or paste HTML source from another editor, then click **OK** to return to the message template window.
8. You can use variables marked with braces { }. To see a list of variables available in any field, type { to open a context menu. You can also enter variable names manually. You can use nested variables. For details of the variables available in templates, see “Using Variables” on page 204.
9. Click **OK**.

## Editing Templates

You can edit a template, including the address information and the message bodies.

### To edit a template:

1. Double-click a template name in the Configurator.
2. Make changes then click **OK**. If you have created both a plain text and a HTML version of the template, remember to change both versions.

## Duplicating Templates

You can make a copy of a template if you want to use it as the starting point for another template.

**To copy a template:**

1. Right-click a template name in the Configurator.
2. Choose **Duplicate** from the context menu.
3. After duplicating the template, make changes to the copy.

## Deleting Templates

You can delete a template if it is not used in any rules.

**To delete a template:**

1. Select a template in the Configurator.
2. Click the **Delete** icon in the toolbar.

## Working with Message Stamps

Message stamps are short blocks of text that MailMarshal SMTP can apply to the top or bottom of an email message body. MailMarshal SMTP message stamps can include a plain text and an HTML version. MailMarshal SMTP will apply the appropriate stamp format to the body text of the same type in the message.

Many companies use message stamps to apply disclaimers or advertising on outgoing email. MailMarshal SMTP can also use a message stamp to notify the recipient that a message has been processed (for example by having an offending attachment stripped).

To work with message stamps in the Configurator, select Message Stamps in the left pane.

**To create a message stamp:**

1. In the left pane of the Configurator, select **Message Stamps**.
2. On the Action menu, select **New Message Stamp**.



3. Enter a name for the stamp.
4. Select whether the stamp is to appear at the top or the bottom of messages.
5. Enter a plain text version of the message stamp in the Plain Text tab.
6. Enter an HTML version of the stamp in the HTML tab. You can apply various formatting, including hyperlinks, to the HTML text using the buttons provided.

To view the raw HTML, right-click in the HTML pane and select **Edit Raw HTML**. Edit the HTML, or paste HTML source from another editor, then click **OK** to return to the message stamp window.

7. To add the new stamp to the list of available message stamps, click **OK**



**Note:** *If message stamping is enabled for RTF (Microsoft TNEF) messages, the plain text message stamp will be used for these messages. To enable RTF stamping, see the Engine Advanced section of MailMarshal Properties.*

Both plain text and HTML message stamps can include the same variables available within email notification templates.

## ***Duplicating Message Stamps***

You can make a copy of a stamp if you want to use it as the starting point for another stamp.

### **To duplicate a message stamp:**

1. Right-click the stamp name in the Configurator.
2. Choose Duplicate from the context menu.
3. After duplicating the message stamp, make any required changes to the copy. Remember to make changes to both the Plain Text stamp and the HTML stamp.

## ***Editing Message Stamps***

You can make changes to a stamp. Remember to make changes to both the Plain Text stamp and the HTML stamp.

### **To edit a message stamp:**

1. Double-click the stamp name in the right hand pane of the Configurator.
2. Make the required changes.
3. Click **OK**.

## ***Deleting Message Stamps***

You can delete a message stamp if it is not used in any rules.

### **To delete a message stamp:**

1. Select the stamp in the right hand pane of the Configurator.
2. Click the **Delete** icon in the toolbar.

## **Using Variables**

When you create a message template, digest template, message stamp, or message classification description, you can use a number of variables. MailMarshal SMTP substitutes the appropriate information when it uses the template or stamp.

Variables are marked by curly braces { }. You can select from available variables in any field where they are available in a template, stamp, or classification. To see a list of available variables in a specific field, type { .

Not all variables are available in all contexts. MailMarshal SMTP may not have the required information to substitute. If MailMarshal SMTP does not have any data, it will enter empty text into the variable marker.

The following table lists commonly used variables and their functions:

Variable	Data inserted
<code>{MessageDigestTableHTML=<i>detail[,option,option,...]}</i></code>	The HTML version of a message digest detail listing. For full information about options, see “Creating Digest Templates” on page 198. See also the variable <code>{MessageDigestTableText}</code> .
<code>{Administrator}</code>	Email address of the administrator as set during post-installation configuration and accessible from the Notifications section of MailMarshal Properties.
<code>{ArrivalTime}</code>	The time when MailMarshal SMTP received a message.
<code>{AttachmentName}</code>	File name of the attached file that triggered a rule condition.
<code>{Date}</code>	The current date. For more information, see “Date Formatting” on page 210.
<code>{DateLastRun}</code>	The date of the previous MailMarshal SMTP message digest for a folder.
<code>{Errorlevel}</code>	The last error returned by a virus scanner or an external command.
<code>{ExternalCommand}</code>	The name of the last External Command used.
<code>{Env=<i>varname</i>}</code>	Inserts the value of a Windows environment variable.
<code>{ExternalSender}</code>	Returns 'y' or 'n' depending on whether the sender was outside or inside the “allowed to relay” space.
<code>{File=<i>fullpath</i>}</code>	Inserts a text file within the body of a message (for instance, can be used to insert the MailMarshal SMTP log for a message in a notification email body).
<code>{Folder}</code>	The name of the folder that is the subject of a MailMarshal SMTP message digest email.
<code>{FolderRetention}</code>	The retention period for a folder that is the subject of a MailMarshal SMTP message digest email.

<b>Variable</b>	<b>Data inserted</b>
{FormattedRecipients}	The recipients of the message, listed in the To: or CC: fields.
{FormattedRecipientsAffected}	Available in Sender templates only. Where a message could not be send to some recipients (in the To: or CC: fields), shows the affected recipients of the message.
{From}	Email address in the 'From' field of the message.
{HasAttachments}	Returns '1' if the message has attachments.
{HelloName}	Name given by the remote email server when MailMarshal SMTP received this message.
{Hostname}	The host name of the server.
{If <i>variable</i> }...[{else}]...{endif}	Allows conditional substitution of text. The condition is true if the variable is not empty. For example: { I f Vi rusName}Thi s message contai ned the vi rus {Vi rusName}. {endi f} The Else clause is optional.
{InitialMessageBody}	The first 200 characters of the body of the message.
{Install}	The install location of MailMarshal SMTP.
{LastAttemptDate}	The date and time of the most recent attempt to deliver the message.
{LastTextCensorRuleTriggered}	The name of the TextCensor Script that was run and the phrase that triggered.
{LocalRecipient}	The message recipient, if any, within the local domains. Includes multiple recipients and CC recipients.
{LocalSender}	The message sender, if any, within the local domains.
{LogName}	The name of the Logging Classification used.
{Message-ID}	Original SMTP Message ID of the message.
{MessageFullName}	Full path to the message file.

Variable	Data inserted
{MessageCount}	The number of messages quarantined for a user in a specific folder and listed in a message digest email.
{MessageDigestTableText}	The plain text version of a message digest detail listing. See also {MessageDigestTableHTML}. <b>Note:</b> The plain text version does not use any detail level or option settings.
{MessageName}	Filename only of the message.
{MessageSize}	The size of the message as originally received.
{MMSmtpMapsRBL}	<b>Note:</b> This variable name is deprecated. Use {ReputationServices}.
{PolicyGroupTitle}	The title of the policy group containing the rule triggered by the message. Replaces {RulesetTitle}.
{RawSubject}	Message subject with any encoding included, as originally received. Use this variable to include the subject in the Subject field of notification templates. See also {Subject}.
{Recipient}	Message recipient. Includes multiple recipients and CC recipients.
{ReleasePassThrough}	Inserts a code recognized by the gateway to release the message applying no further rules. See "Using the Message Release External Command" on page 312.
{ReleaseProcessRemaining}	Inserts a code recognized by the gateway to release the message applying any additional applicable rules. See "Using the Message Release External Command" on page 312.
{RemoteDomainName}	The name of the domain on the remote machine (connecting email server).
{RemoteIP}	The IP of the remote machine.
{ReplyTo}	Email address in the 'Reply to' field of the message.

<b>Variable</b>	<b>Data inserted</b>
{ReputationServices}	A list of Reputation Services (DNS blacklists) that triggered on the message within a Receiver rule. Does not include information generated by the Category Script (SpamCensor) process.
{ReturnPath}	SMTP "Mail From" email address.
{RuleTitle}	The title of the rule triggered by the message.
{Sender}	Email address of the sender. Uses the address in the "From" field unless it is empty, in which case the "Reply to" address is used.
{SenderIDFrom}	The address used for the Sender ID check.
{SenderIDIPAddress}	The IP address used for the Sender ID check.
{SenderIDResult}	The result of the Sender ID check (Pass, Fail, None, SoftFail, Neutral, TempError, or PermError).
{SenderIDReturnedExplanation}	The text explanation returned from the Sender ID query (if any).
{SenderIDScope}	The scope of the Sender ID check (pra or mfrom).
{SenderIP}	IP address of the sender.
{ServerAddress}	Email address used as the 'From' address for notifications as set during post-installation configuration and accessible from the Notifications section of MailMarshal Properties.
{SpamBotCensorResult}	The result string as returned by the SpamBotCensor facility.
{SpamCensorResult}	The result string as returned by the SpamCensor facility.
{SPFExplanation}	The default explanation configured in the SPF Settings window, or the text explanation returned from the SPF query (if any)

Variable	Data inserted
{SsmUrl}	The URL of the MailMarshal SMTP Spam Quarantine Management Website. You can change this value on the Administrator tab of the SQM website.
{StrippedFiles}	The names of any attachment files stripped from the message by rule action.
{Subject}	Message subject, decoded if applicable. Use this variable in most cases. See also {RawSubject}.
{ThreadWorking}	The MailMarshal SMTP working folder name.
{Time}	The current time. See also "Date Formatting" on page 210.
{TimeEnteredQueue}	The time that the message entered the MailMarshal Queue.
{TimeLeft}	The time left to attempt delivering the message in question.
{UnsubscribeUrl}	<p>The URL used to unsubscribe from digests. This variable can be used in digest templates. The variable evaluates blank if a user cannot unsubscribe. Suggested usage:</p> <pre>{if UnsubscribeUrl}To unsubscribe from this digest, use the following link: {UnsubscribeUrl} {endif}</pre>
{VirusName}	Name of the virus detected. This information is only available if the virus scanner being used is a DLL based scanner. If a command line scanner reports a virus this variable is set to "Unknown."
{VirusScanner}	Name of the virus scanner used.

## Date Formatting

When you use dates in variables within message templates, message stamps, and logging classifications, you can include formatted dates. This feature is especially useful to avoid confusion about the order of day, month, and year in dates.

To use date formatting, include the template variable `{date=%%var}` where `var` is one of the sub-variables from the table below. You can include more than one sub-variable within the same date variable. For instance `{date=%%d %%b %%Y}` would return `07 Apr 2004`.



**Notes:** Each sub-variable must be preceded by `%%`. For example, to ensure that the date is formatted according to the Windows locale, use `{date=%%c}`.

- To use locale-specific settings you must ensure that the Windows locale is applied to the account used by MailMarshal SMTP services. For more information, see M86 Security Knowledge Base article Q12670.

The following table lists the available date formatting sub-variables:

Variable	Value inserted
a	Abbreviated weekday name
A	Full weekday name
b	Abbreviated month name
B	Full month name
c	Date and time representation appropriate for locale
d	Day of month as decimal number (01–31)
H	Hour in 24-hour format (00–23)
I	Hour in 12-hour format (01–12)
j	Day of year as decimal number (001–366)
m	Month as decimal number (01–12)



---

<b>Variable</b>	<b>Value inserted</b>
M	Minute as decimal number (00–59)
p	Current locale's A.M./P.M. indicator for 12-hour clock
S	Second as decimal number (00–59)
U	Week of year as decimal number, with Sunday as first day of week (00–53)
w	Weekday as decimal number (0–6; Sunday is 0)
W	Week of year as decimal number, with Monday as first day of week (00–53)
x	Date representation for current locale
X	Time representation for current locale
y	Year without century, as decimal number (00–99)
Y	Year with century, as decimal number
z	Time-zone name or abbreviation; no characters if time zone is unknown

## USING VIRUS SCANNING

You can implement virus scanning as an email policy element. For more information, see “Stopping Viruses” on page 105.



**Notes:** *Anti-spyware scanning (PestPatrol for Marshal and CounterSpy for Marshal) can also be implemented using the same methods. For more information about the value of anti-spyware scanning, see “Anti-Spyware Scanners” on page 340.*

- *Appliance installations are pre-configured using McAfee for Marshal. Appliance installations cannot currently use other scanners.*

## USING EMAIL FOLDERS AND MESSAGE CLASSIFICATIONS

MailMarshal SMTP uses a Microsoft SQL Server database to log basic information about each message it has processed. This information includes the sender, recipient, message size, and actions taken.

If MailMarshal SMTP moves or copies a message to a folder, it logs this event in the database.

Using Message Classifications is another way to add detail to the log records. You can add Message Classifications by including an action within a MailMarshal SMTP standard rule. MailMarshal SMTP Reports, the Console Message History, and the Console search results can show the classification of a message.

You should include at least one logging action (either a folder action or a classification action) in each standard rule. MailMarshal SMTP default rules include such actions.



**Notes:** *To avoid confusion in reporting, MailMarshal SMTP will not allow a folder and a classification with the same name.*

- *If a folder or classification is related to spam or virus activity, you should add it to the appropriate reporting group. For more information about reporting groups, see “Configuring Reporting Groups” on page 319.*

## Working with Message Classifications

Message classifications are useful for reporting on broad categories, such as viruses or executable files quarantined. You can also use classifications to record very specific occurrences such as a specific file or size of file being sent. For example you could answer the question “How many PDF files over 500K in size are sent by Sales each week?” by creating a rule to log sending of such files. If several rules place messages in a single MailMarshal SMTP folder, you can use classifications to give additional granularity for searching and reporting.

To work with Message Classifications in the Configurator, select Message Classifications from the left pane menu tree.

### To create a message classification:

1. On the Action menu, choose **New Message Classification**.
2. In the window, enter a meaningful name for the classification.
3. Give a brief description of the classification and its purpose. This description will be used in the Console and Reports, and can contain { } variables as in message stamps and templates.
4. To add the classification, click **OK**.

## ***Editing Message Classifications***

You can edit the name and description of a classification.

### **To edit a message classification:**

1. Double-click the classification name in the right pane of the Configurator to view its properties.
2. Make any required changes.
3. Click **OK**.

## ***Duplicating Message Classifications***

You can make a copy of a classification if you want to use it as the starting point for another classification.

### **To duplicate a message classification:**

1. Right-click the classification name in the Configurator.
2. Choose **Duplicate** from the context menu.
3. After duplicating the classification, make any required changes to the copy.

## ***Deleting Message Classifications***

You can delete a classification if it is not used in any rules.

### **To delete a message classification:**

1. Select the classification name in the right pane of the Configurator.
2. Click the **Delete** icon in the toolbar.

## Working with Folders

MailMarshal SMTP uses folders to store messages that it has quarantined, parked for later delivery, or archived. You can delete quarantined messages, release them to the recipient, and manage quarantined messages in other ways.

You can configure folders with specific security settings. You can configure folders to be available for end-user management through the Spam Quarantine Management console. You can configure folders to allow “fingerprinting” of released messages.



**Note:** *In earlier versions of MailMarshal SMTP you could configure the default action that MailMarshal took if a message was released from a folder. This option has been replaced by the “release action” option in rule actions. For more information, see “Copy the message” on page 160 and “Move the message” on page 166.*

MailMarshal SMTP includes predefined folders that address common email security issues and automatically categorize quarantined mail. MailMarshal SMTP provides many predefined folder types, including folders that:

- MailMarshal SMTP uses to categorize various types of attachments
- MailMarshal SMTP uses to categorize various types of policy breaches
- SpamCensor uses to categorize various types of spam
- MailMarshal SMTP uses to categorize suspected and confirmed virus-infected email
- Hold messages that MailMarshal SMTP cannot process or cannot deliver, called dead letters. Dead Letters can result from bad email addresses, from corrupted data, from differing interpretations of Internet standards, or when a message is intentionally malformed in an attempt to exploit a security vulnerability.

Predefined and newly-created folders have default properties that you can modify. For example, the default setting on the Attachment Type-Executables folder does not allow you to save stored messages to another location.

If existing MailMarshal SMTP folders are not appropriate for your needs, modify the properties of an existing folder or create your own folders.

## Creating Folders

You can create as many folders as your policy requires. You can create the following types of folders:

### Standard Folder

Used to quarantine dangerous or suspect mail. You can specify that an administrator or regular user can manage the folder contents. You can specify that messages released from the folder are eligible for attachment fingerprinting.

### Archive Folder

Used to keep historic copies of delivered mail. MailMarshal SMTP saves messages stored in the folder for a specific period of time. You cannot manually delete mail stored in an archive folder. You can specify that messages released from the folder are eligible for attachment fingerprinting.

### Parking Folder

Used to delay the delivery of mail. MailMarshal SMTP releases messages stored in the folder according to a predefined schedule.

### To create a folder:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Policy Elements > Folders**.
2. On the **Action** menu, click **New Folder**.
3. Specify the appropriate values. For more information about fields on a window, click **Help**.
4. Click **Finish**.

## Editing Folders

You can change the name, security permissions, and most features of a folder. You cannot change the type of an existing folder.

### To edit a folder:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Policy Elements > Folders**.
2. Select the folder you want to modify.
3. On the **Action** menu, click **Properties**.
4. On each tab, specify the appropriate values. For more information about fields on a window, click **Help**.
5. Click **OK**.

## *Deleting Folders*

You can delete a folder if it is not used in any rules.

### To delete a folder:

1. In the right pane of the Configurator, select the folder name.
2. Click the **Delete** icon on the taskpad header or the toolbar.

Deleting a folder in the Configurator deletes only the link to the folder that appears in the Configurator. This action does not delete the physical folder or any email messages it contains. To delete email messages use the MailMarshal SMTP Console. To delete the physical folder and its contents use Windows tools.

# HEADER MATCHING AND REWRITING

MailMarshal SMTP can perform searches and replace text in email headers using a Regular Expression engine. You can apply rewriting globally when messages are received. You can also perform header searches and header replacements within standard rules.

**Warning:** *Regular Expression matching and substitution provides very powerful capabilities. However, regular expressions are complex and can be difficult to construct. If headers are rewritten incorrectly, you may be unable to determine the sender or intended recipient of affected messages. Use this facility with care.*

## Changing and Adding Headers with the Receiver

MailMarshal SMTP provides global header rewriting to modify email header and envelope detail. Global rewriting is typically used to allow email aliasing. This action is performed by the MailMarshal SMTP Receiver during email message receipt.

Some examples of actions that can be performed are

- Address modification: for example, changing user@host.domain.com to user@domain.com.
- Field removal: for example, stripping out the received: lines from outbound messages.
- Alias substitution: for example, replacing addresses via a lookup table, as in user1@olddomain.com being replaced by user2@newdomain.com.
- Domain masquerading: for example, replacing all addresses in thisdomain.com with identical addresses in thatdomain.com.



### To work with global header rewriting:

1. On the Tools menu of the Configurator, select **MailMarshal Properties**.
2. On the MailMarshal Properties window, select **Header Rewrite** from the left pane. You can add a new global header rewrite rule, edit an existing rule, or delete an existing rule. You can also change the order of evaluation of the rules. For details of the rule editing processes, see “Using the Header Rewrite Wizard” on page 220.

## Using Rules to Find Headers

You can search email headers using regular expressions using the MailMarshal SMTP standard rule condition “Where message contains one or more headers.” This rule condition allows matching based on the presence of specific email message headers, or specific content within any header.

To create a header match condition, in the rule condition window click **New**.

To perform more than one header match within a single condition, complete the match rule wizard for each match.



**Note:** *If more than one header to match is entered within a single rule condition, all expressions must match for the condition to be true (logical AND). To check any of several headers (logical OR), use one rule per header.*

For details of the rule editing processes, see “Using the Header Rewrite Wizard” on page 220.

## Using Rules to Change Headers

You can alter email headers using regular expressions using the MailMarshal SMTP standard rule action “Rewrite message headers using expressions.” This rule action allows matching based on the presence of specific email message headers, or specific content within any header.

To create a header rewrite action, within the rule action window click **New**.

To perform more than one header rewriting action within a single condition, complete the rule wizard for each header rewriting action.



**Note:** *If more than one header to rewrite is entered within a single rule, the order in which rewriting is applied will be significant. Rewriting actions will apply in top down order as they are listed in the rule action window. To change the order, use the arrows in the window.*

For details of the rule editing processes, see “Using the Header Rewrite Wizard.”

## Using the Header Rewrite Wizard

This wizard allows you to create a header matching or header rewriting rule. The wizard uses regular expression matching and substitution. For more information about regular expressions, see “Regular Expressions” on page 331.

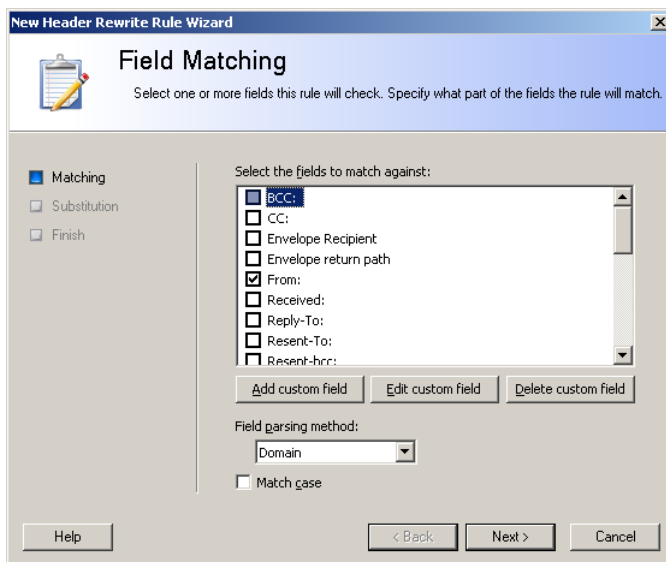
The windows of the wizard are as follows:

- An introduction page that gives warning information (shown for Rewriting only).
- A field matching page to select the header or envelope fields to be matched, and the portion of the field to be modified.
- A substitution options page where matching and substitution expressions are entered.
- A naming and test page for naming the rule and testing the matching and substitution.


You can also change the order of evaluation of header rewriting rules using the arrows at the bottom of the parent window.

## To use the Header Wizard:

1. Select the fields that you want the rule to apply to from the list. You can add or edit a custom header field name using the buttons provided.



2. Choose a parsing method from the list. Depending on this selection, MailMarshal SMTP will apply regular expression matching to parts or all of the selected headers.

 **Note:** To insert a custom header, use the parsing method “Entire Line.” To match or modify all email addresses, use the method “Email Address”.

- If you select the method “Entire Line” MailMarshal SMTP will use the entire text of the header as the input text for the substitution engine.
- If you select the method “Email Address” MailMarshal SMTP will use each email address found in the line as the input text.
- If you select the method “Domain” MailMarshal SMTP will use the domain part of each email address as the input text.

3. Select the check box **Match Case** to perform a case sensitive search.  
Clear the check box to make the search case insensitive.



**Note:** To search for email addresses or domains, use a case insensitive search.

4. Click **Next** to proceed to the Field Substitution window.

The screenshot shows the 'New Header Rewrite Rule Wizard' dialog box, specifically the 'Field Substitution' step. The title bar reads 'New Header Rewrite Rule Wizard'. The main title is 'Field Substitution' with a subtitle 'Enter details of the rewriting action the rule will take.' On the left, there are three radio buttons: 'Matching' (checked), 'Substitution' (checked), and 'Finish' (unchecked). The main area contains several options:
 

- 'Optional exclusion filter' (unchecked) with an empty text field.
- 'Field search expression:' (checked) with a text field containing '\*.\*,example.com'.
- 'Substitute into field using expression:' (checked) with a text field containing 'example.com'.
- 'Map using file:' (unchecked) with sub-fields for 'File name:' and 'Lookup key:'.
- 'Delete the field' (unchecked).
- 'Insert if missing:' (unchecked) with an empty text field.

 At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

5. In the **Optional Exclusion Filter** field, you can enter a regular expression. If this expression is found in the input text, the search will return “not matched”.
6. In the **Field Search Expression** field, enter a regular expression that MailMarshal SMTP should use to select the data for matching or rewriting. If the input text matches this expression, the rule will match or rewrite it, subject to exceptions based on the exclusion filter.

7. If this is a rewriting rule, choose one of the rewriting methods:

- **Substitute into field using expression** replaces the matched data using a sed or Perl-like syntax. You can use sub-expressions generated from the field search here. Refer to the sub-expressions as \$1 through \$9.



**Note:** If you replace the entire contents of a field, be sure to terminate the text with a CRLF (`\r\n`). You can insert this value through the arrow to the right of the field. If you enter `$0` (the tagged expression containing the entire input line) at the end of the substitution expression, a CRLF will already be included.

- **Map using file** provides for substitutions from a file, to allow a level of indirection in resolving what to substitute into the field. See “Regular Expressions” on page 331.
- **Delete the field** removes the matching material from the header. When **Entire line** is selected in the parsing options, selecting Delete the field removes the entire header line from the message.
- **Insert if missing** permits you to add a new header if any of the selected headers does not exist. MailMarshal SMTP will use the text of this field as the value of the new header line. For instance if you have added the custom header `x-MyNewField` then you might enter the value Created by Header Rewrite.

8. Click **Next** to proceed to the Rule Completion window.

**New Header Rewrite Rule Wizard**

**Header Rewrite Rule Completion**

Specify a name and description for this rule. Test the rule action before enabling changes.

Matching  
 Substitution  
 Finish

Type the name of the rule:  
Remove internal server name

Enable field changes  
 Log changes

Comment:  
This rule removes internal server names from all From headers

Test Rule  
Source: joe@internalserver.example.com <joe@internalserv  
Result: joe@example.com <joe@example.com><end>

Test

Help < Back Finish Cancel

9. Enter a name for the rule.

10. Optionally enter a comment to explain the purpose of the rule.

11. To test the rule, enter an input string in the **Source** field and click **Test**. The result will appear in the **Result** field. For rewriting actions, the result will be the rewritten string. For matching, the result will be “matched” or “not matched”.

12. **If this is a rewriting rule**, select whether the changes will be actually applied and/or logged. Select the check box **Enable field changes** to apply this rule to messages. Select the check box **Log changes** to write a log of changes to the MailMarshal SMTP logs for the message. If only **Log changes** is selected, the logs will show the changes that would have occurred.
13. Adjust the order of evaluation using the arrows provided below the list of rules.



**Notes:** *If you use several header matching rules within a single standard rule condition, all must evaluate true for the condition to be true.*

- *If you create several rewriting rules for global Header Rewrite or within a single standard rule action, the order of evaluation will be significant. Rewriting actions will be applied in top-down order as shown on the window.*

## EXTENDING FUNCTIONALITY USING EXTERNAL COMMANDS

An external command is a custom executable, Windows command, or batch file that can be run by MailMarshal SMTP. The command can be used to check email messages for a condition, or to perform an action when a message meets some other condition.

You can use custom executable files or batch files with the standard rule condition “Where the external command is triggered.” For instance, you can invoke `fgrep.exe` for advanced expression matching.

If you want to use an external command to check for a condition, the command must return a standard return code.

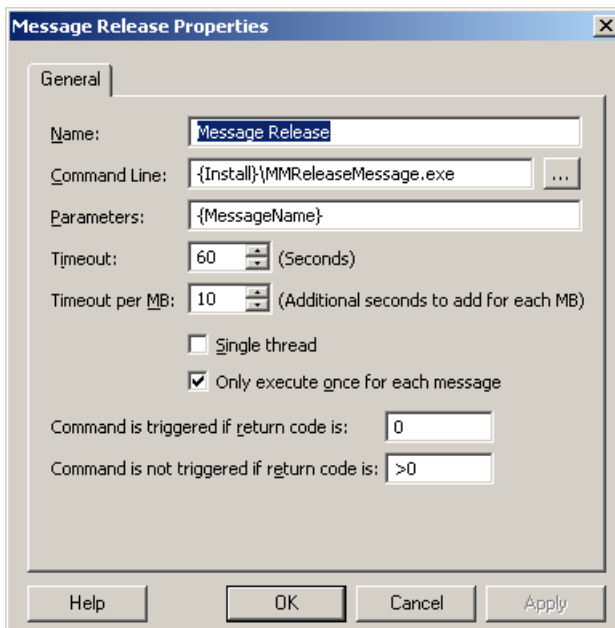
You can also use custom executable files with the standard rule action “Run the external command.” For instance, a particular email subject line could trigger a batch file to start or stop a system service, or to send a page or network notification to an administrator.

MailMarshal SMTP is provided with an external command for message release. See “Using the Message Release External Command” on page 312.

To use an external command in MailMarshal SMTP rules, you must first define it.

**To create a new external command definition:**

1. In the left pane of the Configurator select **External Commands**.
2. On the Action menu, click **New External Command** to open the External Command window.



3. Enter a name for the external command.



4. Type the path for the executable file. You can also browse for the file by clicking **Browse**.



**Note:** To use a batch file, you must invoke the command interpreter explicitly as follows:

```
%Systemroot%\system32\cmd.exe /C {batchfile.cmd} [variables...]
```

5. In the **Parameters** field, enter any command line parameters necessary for the command. You can pass specific information about a message to the command using MailMarshal SMTP variables.
6. The **Timeout** and **Timeout per MB** values control how long MailMarshal SMTP will wait for a response before ignoring the external command. The default values are very generous.



**Note:** If the external command executable uses 10% of the timeout time in actual processing (CPU usage), MailMarshal SMTP will terminate the command, log the event as a runaway process, and place the message in the *Dead Letter\Unpacking* folder.

7. The **Single Thread** setting indicates whether the command must operate on one message at a time, or can be invoked multiple times. In most cases this box should be left selected. You can multi-thread certain executable files.
8. The **Only execute once for each message** setting determines whether an external rule condition command will be run for each component of a message, or only once. For example if you are using fgrep to perform Regular Expression searches of attached files, this box should be cleared to ensure that MailMarshal SMTP passes each component of each message to fgrep.exe.
9. If you plan to use the external command as a rule condition, you must set the trigger return code information. You should find this information in the documentation of the executable.

Two fields allow you to enter trigger values which further specify the meaning of the code returned from the virus scanner.

- If the code returned matches any value entered in the field **Command is triggered if return code is**, MailMarshal SMTP will consider the condition to be satisfied.
- If the code returned matches any value entered in the field **Command is not triggered if return code is**, MailMarshal SMTP will consider the condition not to be satisfied.
- If the code returned matches neither field, the file is moved to the Undetermined dead letter folder and an email notification is sent to the MailMarshal SMTP administrator.
- Entries in both return code fields can be exact numeric values, ranges of values (for example 2-4), greater than or less than values (for example <5, >10). More than one expression can be entered in each field, separated by commas (for example 1,4,5,>10).

## CONFIGURING REPUTATION SERVICES

MailMarshal SMTP can retrieve information from DNS based blacklists or Reputation Services, including the Marshal IP Reputation Service and third-party services such as SpamCop and SpamHaus.

Configuring a DNS Blacklist for use in MailMarshal SMTP is a two step process. You configure details of the list in Policy Elements, then you configure one or more receiver rules to filter email based on the list information

For more information about configuring Reputation Services, see “Controlling Who Can Send Email Through Your Server” on page 111. For details of the information on the Reputation Services window of the Configurator, see Help.

---

## Chapter 8

# Monitoring Email Flow

MailMarshal SMTP provides a number of tools to assist in daily administration of email flow and server health. These include the Console and Web Console, the Configurator, MailMarshal SMTP Reports, the Spam Quarantine Management Website, Windows event logs, the Windows performance monitor, and the text logs generated by each MailMarshal SMTP service.

You can delegate access to a number of these tools, including the Console functions, reports, and spam management.

<b>If you want to:</b>	<b>Use:</b>
View a summary of email traffic and filtering activity for the current day or other period; view details of configuration update status and running MailMarshal SMTP services for each email processing server	The Dashboard page in the Console. See "Viewing Server Statistics" on page 232.
View totals of messages processed and queued for each email processing server; delete a message queued for sending	The Servers item in the Console. See "Deleting and Retrying Queued Messages" on page 234.
View a history of service alerts (unusual activity) for all MailMarshal SMTP servers	The Alert History in the Console. See "Viewing Alert History" on page 245.
Stop and start MailMarshal SMTP services	The Servers and Arrays item in the Configurator. See "Managing Node Services" on page 282.
View details of each message processed	The Email History and Folders in the Console. For more information, see "Viewing Email History" on page 243.

<b>If you want to:</b>	<b>Use:</b>
Search for details of a specific message	The History Search in the Console. For more information, see “Searching Folders and Email History” on page 244.
View, release, redirect, or delete a message in quarantine; report a message to M86 as spam or not spam (if incorrectly classified)	The Email History, History Search, and Folders in the Console.
View a graphical display of performance information for the MailMarshal SMTP services	The Windows Performance monitor. For more information, see “Performance Monitor” on page 254.
View detailed debugging information for the MailMarshal SMTP filtering and delivery services	The Windows Application log and the MailMarshal SMTP text service logs on each server. For more information, see “Viewing Event History” on page 250 and “Using MailMarshal SMTP Text Logs” on page 255.
Generated detailed reports on email traffic and filtering activity over time	MailMarshal SMTP Reports. For more information, see “Generating Reports” on page 320.
Delegate administrative functions to help desk personnel	Console Security on the MailMarshal Properties window and the folder security options for each folder, all found in the Configurator. For more information, see “Setting Console Security” on page 246.
Delegate management of spam and other quarantined messages to email users	The Spam Quarantine Management Website and the properties of folders. For more information, see “Setting Up Spam Quarantine Management Features” on page 304.

# USING THE MAILMARSHAL SMTP CONSOLE

The Console provides summary information on the current state of MailMarshal SMTP, as well as administrative access to the quarantine folders and message sending services. The Console also provides access to support news and updates from M86 Security. You can install the Console on any workstation that can connect to the MailMarshal SMTP Array Manager on port 19001 (or whatever port you have configured at the Array Manager).

You can also access nearly all Console features using the MailMarshal SMTP Web Console. The Web Console installs as a virtual directory under Microsoft IIS and can be accessed from any computer that can browse to the server where the Web Console is installed. All functions of the Console are also available in the Web Console unless otherwise noted.

The procedures in this chapter refer to the MailMarshal SMTP Console MMC application. The Web Console provides the same left pane items, but the Web interface uses different control buttons and menus. For details of how to perform specific tasks using the Web Console, please see the Help for the Web Console.



**Note:** You can limit access to the Console and to specific folders by granting privileges to specific Windows accounts. For more information see “Setting Console Security” on page 246.

## Connecting to MailMarshal SMTP Using the Console

You can connect using the Console from any computer that can connect to the Array Manager computer.

### To connect using the Console:

1. Start the MailMarshal SMTP Console from the MailMarshal program group.
2. Choose the name of the Array Manager server from the list, or browse the network for a server by clicking **Browse**.

3. If the Array Manager server expects connections on a port other than the default 19001, enter the correct value. (To change this value at the Array Manager, use the MailMarshal SMTP Server Tool. See “Working with Array Communications” on page 294.)
4. To connect as a user other than the current Windows user, select the appropriate radio button then enter the user information.
5. To attempt to connect, click **OK**.

## Connecting to MailMarshal SMTP Using the Web Console

You can connect using the Web Console from any computer that can browse to the Web Console server.

### To connect using the Web Console:

1. Open Internet Explorer and browse to the Web Console Website you have configured.
2. On the login page of the Web Console site, enter the connection details for the Array Manager, and a user name that has permission to connect to the Console.

## Viewing Server Statistics

The Dashboard page in the Console (previously titled MailMarshal Today) provides basic information about MailMarshal SMTP at a glance. To view the Dashboard, in Taskpad View select MailMarshal SMTP Console in the left pane. You can select the period shown in the graphs using a menu at the top of the page. (To switch to Taskpad View, on the View menu, click **Taskpad View**.)

Information available on this page includes the following items:

**Server Summary**

Lists the MailMarshal SMTP email processing servers, and shows the software version as well as the last time you committed changes to the configuration and the last time you restarted the services associated with each server. Also shows any stopped MailMarshal SMTP services and selected other problems on each server.

**Mail Statistics**

Shows the number of messages and volume of traffic for a selectable period, divided into inbound and outbound traffic. Inbound traffic is email addressed to the local domains as configured in MailMarshal SMTP. Mail Statistics also shows the total number of messages currently in the MailMarshal SMTP quarantine.

**Threats and Malicious Content**

Shows the number of messages that MailMarshal SMTP has classified as spam, virus infected, or Blended Threat related (containing malicious URLs). The data can include one or more folders or message classifications. For more information about how to view or edit the list of data included, see “Configuring Reporting Groups” on page 319.

**Threat Metrics**

Shows the number of items that MailMarshal SMTP has scanned for viruses, and the number of URLs checked for Blended Threats.

**Top Quarantine Folders**

Shows details about the top five quarantine folders, ranked by the number of messages they contain. The Percentage of Messages Processed statistic can exceed 100%. MailMarshal SMTP might classify a message in more than one spam folder, and count the duplicate copies when generating Top Quarantine Folders statistics, resulting in a count that exceeds 100%. You can disable Top Quarantine Folders statistics from the Reporting section of MailMarshal Properties in the Configurator.

### Mail Transport Policies

Shows the number of messages processed in the selected period that triggered MailMarshal SMTP transport policies. Transport policies cause a message to be refused by MailMarshal SMTP.

MailMarshal SMTP blocks messages that trigger transport policies before message delivery. These messages are not quarantined. **Mail Transport Policies** also shows the number of refused relay attempts and the number of servers blocked by DHA and DoS attack prevention.

### Product Information

Shows MailMarshal SMTP user license information and SpamCensor updates.

The Servers item collects server and service status information for each MailMarshal SMTP email processing server. To view this item click **Servers** in the left pane. For each server the Console shows the server name, version of MailMarshal SMTP installed, whether the configuration is up to date with the configuration committed at the Array Manager, and whether the services are running.

For each server, you can also see details about the associated services and processed messages, as well as details of free disk space and event logs. To see a summary of the Receiver and Sender activity for a specific server, expand the **Servers** item then expand the item for the server name. To see details of the individual processing tasks, select an item (**Receiver**, **Sender**, or **Domains**). For more information see Help.

## Deleting and Retrying Queued Messages

The **Sender** item for each server shows the messages MailMarshal SMTP is currently sending. The **Routes** item for each server shows a list of the route table entries that MailMarshal SMTP is attempting to send messages to, including items that are pending a retry.



You can stop sending a message that MailMarshal SMTP is currently sending and delete it. In the Sender view, highlight the message, and click **Kill Message**.

To attempt to send all messages queued for a specific route entry in the queue, in the Domains view, highlight a domain and click **Retry Route Now**.

The **Hold Queues** item for each server shows the number of items that are being held for each rule with a “Hold” action. To retry the rules, click **Retry Now**.

## Viewing Folders and Folder Contents

MailMarshal SMTP message quarantine folders include the archive, parking and standard folders into which messages are placed through rule action, as well as the Dead Letter folders used for messages that cannot be processed, and the Mail Recycle Bin used to hold deleted items for a period.

To view a list of MailMarshal SMTP message quarantine folders, expand the menu item **Folders**.

To view the contents of a folder, select it in the left pane. The contents will be displayed in the right pane, divided into daily subfolders. Select a daily folder to see its contents. By default no more than 200 items will be retrieved for each subfolder per screen. You can view the next or previous screen using the Page Up and Page Down keys. You can adjust the number of items per screen by choosing **Preferences** from the Tools menu. You can sort the items on the screen by clicking column headers.



**Note:** *The column sorting function only sorts the items on the current screen. If the folder contains more than one screen of items, sorting does not sort over multiple screens. Use the user filter at the top of the listing, or the search function, to retrieve a limited number of items.*

You can also view items in the folders using the Email History view and the Search window.

## Working With Email Messages

You can perform the following actions on an email message located in a MailMarshal SMTP quarantine folder:

### View

Open a new window displaying the message headers, body, attachments, and the MailMarshal SMTP email processing logs if they are available for the message.

### Forward

Send a copy of the message to a specified email address.

### Delete

Move the message to the MailMarshal SMTP Mail Recycle Bin, or optionally delete it permanently. You cannot perform this action for items in Archive folders.

### Release

Queue the message for action by other MailMarshal SMTP services. This action is typically used to deliver a quarantined message to the original recipient. You can choose from several options.

### Report Spam

Forward a copy of the message to M86 tagged as “spam.”

### Report Not Spam

Forward a copy of the message to M86 tagged as “not spam.”



**Note:** Use the Spam and Not Spam options to help improve MailMarshal SMTP spam detection by reporting messages that were wrongly classified. The messages you send are automatically processed. M86 treats the messages in complete confidence.

- To report a message you must have permission to forward messages from the folder that contains it. To configure permissions on a folder, see “Editing Folders” on page 217.

To work with a message, select it in the Email History, the Message Search results, or the Folders view.

## ***Forwarding Messages***

Use forwarding to send a copy of the message to a specified email address.

### **To forward a message:**

1. Select the message.
2. Click the **Forward** icon on the toolbar, or open the message then choose **Forward** from the Message menu.
3. Enter one or more addresses. To forward to multiple addresses, enter them separated by semi-colons (for instance Ri chardN@exampl e. com; Geral dF@exampl e. com).
4. By default MailMarshal SMTP retains the message when you forward it from a quarantine folder. To adjust this behavior select or clear the check box. MailMarshal SMTP will not delete messages from archive folders.

## ***Deleting Messages***

Deleting a message sends it to the Mail Recycle Bin, or optionally deletes it permanently.

### **To delete one or more messages:**

1. Select the messages. You can use shift and control click to multi-select.
2. Click the **Delete** icon in the taskpad header. The message(s) will be sent to the Mail Recycle Bin folder.
3. ***If you want to delete the message(s) permanently***, hold down the Shift key while clicking the **Delete** icon.

## ***Restoring Messages***

Once MailMarshal SMTP places a message in a quarantine folder, it retains that message for the period configured in the properties of the folder, unless you choose to delete the message permanently.

The retention period applies even if the message is moved to the Mail Recycle Bin or restored. For instance, if the Spam folder has a retention period of one week, and MailMarshal SMTP moves a message to the Spam folder, then you delete it to the Mail Recycle Bin, it will be permanently deleted from the Mail Recycle Bin one week after it was first received.

Restoring a message retrieves it from the Mail Recycle Bin. MailMarshal SMTP displays it in the folder where it was originally quarantined.

**To restore one or more messages from the Mail Recycle Bin to their original location:**

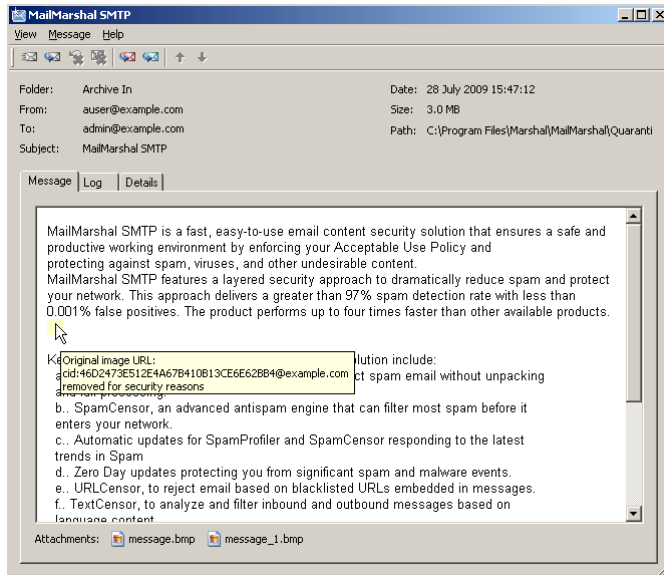
1. Select items in the Mail Recycle Bin.
2. Click the **Restore** icon.

### ***Viewing Messages***

View a message to display the message headers, body, attachments, and the MailMarshal SMTP email processing logs if they are available.

To view a message and its associated processing log in a folder, History, or Search view, double-click the message.

MailMarshal SMTP opens the message in a new window.



The title of the window shows the message subject. The body of the window shows basic information about the message and any attachments.

The lower portion of the message window includes three tabs: Message, Log, and Details. The Message and Details tabs restrict access to items that could represent security threats. Large images may be converted to thumbnails for performance reasons.

### Message

Shows the message body in the richest available format (HTML, RTF, or plain text).

### Details

Shows a tree view of the components of the message. You can click any item to view it in detail.

## Log

Shows the MailMarshal SMTP processing log for the message.

The processing log is only available if it was copied by the rule that placed the item in the folder. It is good practice, especially for debugging purposes, to copy the log for each message. If the rule does not copy the log information, you may be able to retrieve it from the main MailMarshal SMTP text logs. The text logs are created by default in the Logging subfolder of the MailMarshal SMTP installation folder. However by default these logs are only retained for five days.

You can copy message text to the Clipboard from any of the message tabs. Use the following task to copy text. MailMarshal SMTP does not support copying with Ctrl-C for this task.

### To copy message text to the Clipboard:

1. Open a message.
2. Select the tab from which you want to copy text.
3. Select the text you want to copy.
4. Right-click and select **Copy**.

## Releasing Messages

Releasing a message queues it for action by other MailMarshal SMTP services.

To release a message, select one or more messages, and then click **Release Message(s)**.

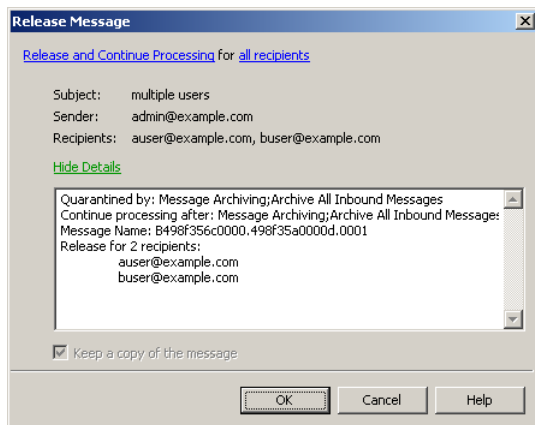


**Notes:** You can also release messages using a specially formatted email message. See “Using the Message Release External Command” on page 312.

- You can add “fingerprints” of attached files into a list that MailMarshal SMTP can use in Rules. For more information, see M86 Security Knowledge Base article Q10543.

By default the messages will be released for all recipients. By default the messages will be processed through additional rules, as specified for each message in the rule that placed the message in a folder.

**To review the release actions and recipients**, on the Release Message window click **Show Details**. To hide the additional information, click **Hide Details**.



**To change the release actions:**

1. On the Release Message window, click the link **Release and Continue Processing** (the link text will be different if you have already changed the action).
2. Choose from the following actions:

#### **Continue processing the message**

This option continues processing the messages as specified for each message in the rule that placed the message in a folder. This is the default action. This action can be used to release a message from quarantine while testing it for any further violations of policy.



**Note:** *If rules change after the message is placed in the folder, MailMarshal SMTP may not be able to perform the requested action. For more details, see Help for this window.*

### **Reprocess the message**

This option resubmits the message for processing by the current set of MailMarshal SMTP rules. This option can be useful to resubmit a number of messages after rules have been adjusted.

### **Pass the message through**

This option queues the message for delivery with no further evaluation.

### **Add attachment fingerprints**

The unique “fingerprint” of each attachment will be loaded into the MailMarshal SMTP configuration and will be available on all email processing servers in the array. The list of “valid fingerprints” can be used in a rule condition.

You can choose to add the fingerprints of all attachments to a message, or only image attachments. MailMarshal SMTP automatically deletes a fingerprint and the associated file if it does not trigger a condition for six months.

This option is available only if enabled for the folder where the message is stored. For more information about enabling the option, see “Editing Folders” on page 217. For more information about attachment fingerprints, see “Where attachment fingerprint is/is not known” on page 140.

### **Report as not spam**

Forward a copy of the message to M86 tagged as “not spam.” To report a message you must have permission to forward messages from the folder that contains it. For more information about configuring permissions on a folder, see “Editing Folders” on page 217.



### To change the release recipients:

1. On the Release Message window, click the link **all recipients** (the link text will be different if you have already selected recipients).
2. The Select Recipients window shows all recipients of the message. To remove a recipient, clear the box for that recipient.



**Note:** *This option is only available when you release a single message.*

The following additional option is available:

#### **Keep a copy of the message**

Once MailMarshal SMTP has completed the selected actions, by default it deletes the message from the folder (except archive folders). Check this box to retain the message in the folder

If the message has multiple recipients and you have chosen not to release it for all users, MailMarshal SMTP removes the users who received the message from the list of message recipients. In this case, if you select **Keep a copy**, MailMarshal SMTP keeps all existing users on the list. MailMarshal SMTP only deletes the message from a folder when it has no remaining recipients.

## Viewing Email History

The Email History view shows each action taken on each message. Actions can include message classifications, moving to folders, delivery, and delivery failure among others. MailMarshal SMTP usually creates more than one history record for a specific message. If a history record records a move or copy to a folder and the message is present in the folder, you can use it to process the message exactly as you could from the folders view

By default no more than 200 items will be retrieved per screen. You can view the next or previous screen using the Page Up and Page Down keys. You can adjust the number of items retrieved by choosing **Preferences** from the Tools menu. You can sort the items on the screen by clicking column headers.



**Note:** *The column sorting function only sorts the items that have been retrieved. If there is more than one screen of history, sorting does not sort over multiple screens. Use the user filter at the top of the listing, or the search function, to retrieve a limited number of items.*

## Searching Folders and Email History

You can limit the items displayed in the folders or email history using the User Filter field at the top of the listing in Taskpad view. You can use wildcard characters in this field. For more information about syntax, see “Wildcard Characters” on page 329.

Search the folders or email history by choosing **Search** from the Action menu. You can choose from a large number of search criteria including dates, subject, classification, and email addresses. If you want to see only items that can be viewed and processed, expand **Where can the message be found** on the Search for Messages window to search only for items in specific folders.

You can search using any combination of the following options:

### **What is the Message Name**

Allows you to enter a unique name MailMarshal SMTP has assigned to this message. MailMarshal SMTP includes this information in the headers of each message. You can enter the name alone (13 characters), or the name and edition (13.12 characters) to identify a specific edition of the message. You can add the server ID (13.12.4 characters). You cannot combine this option with any other option.

### **Where can the message be found**

Allows you to select a folder, or “all messages” to search all folders and classifications.

**When did the message arrive**

Allows you to select the time and date when an action was logged. You can also enter a range of dates. For instance, you can use this option to search for messages that were sent on a specific day.

**What is the email address**

Allows you to enter the address the message was sent to, from, or both. You can use wildcard characters. For more information about wildcard character syntax, see “Wildcard Characters” on page 329.

**What text does the subject contain**

Allows you to find messages containing certain text in the subject line. You can use wildcard characters. For more information about wildcard character syntax, see “Wildcard Characters” on page 329.

**How was the message classified**

Allows you to select a specific MailMarshal SMTP classification. Classifications include both user classifications and system classifications such as “Delivered successfully”.

**What size is the message**

Allows you to specify a size or range of sizes.

**Search history items**

Allows you to select whether the search will return message history records including classifications, system actions, and messages that have been quarantined within the database retention time, or only show messages currently in folders.

## Viewing Alert History

MailMarshal SMTP generates alerts for specific events of interest. Some of the events included are services starting, stopping, or remaining idle for a longer than expected time.

To view a historical list of service alerts, select **Alert History** in the left pane.

## Setting Console Security

MailMarshal SMTP Console uses the Windows secure remote procedure call (RPC) mechanism to communicate with the MailMarshal SMTP Array Manager server. A Console user must have an account and password that the Array Manager Server can validate. If the Console workstation is in a different domain from the Array Manager server, you can either set up a trust relationship or create local accounts on the Array Manager server. If the Console and the server are separated by a firewall (for instance if the server is located in a DMZ), port 19001 must be opened in the firewall to allow remote Console access.



**Note:** *If the Console workstation is in a different domain from an Array Manager server on a computer running Microsoft Windows 2003, M86 Security recommends that you use a trust relationship, rather than creating local accounts.*

You can permit or deny access to each feature of the Console for each user or group. You can also set access to view and act on the contents of each quarantine folder.

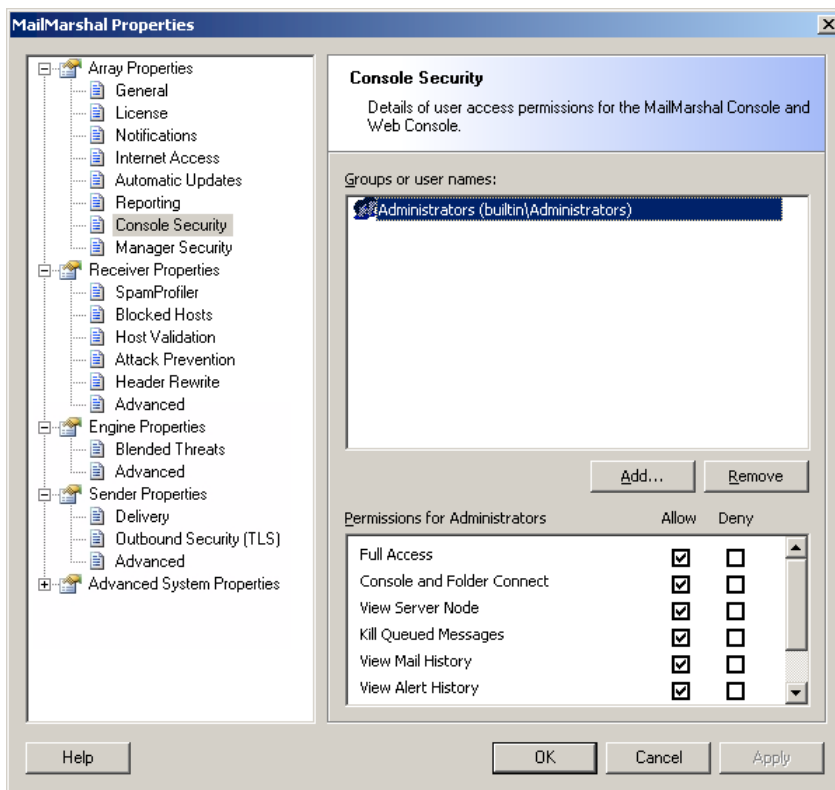
### **Configuring Console Access**

Set Console access permissions to control which users can use various views available in the MailMarshal SMTP Console.

#### **To configure access to Console features:**

1. Open the MailMarshal SMTP Configurator.
2. On the Tools menu, select **MailMarshal Properties**.

3. Select **Manager Security** from the left pane. The display shows a list of users and groups with permission over the Console features. By default all members of the Windows Administrators group on the MailMarshal SMTP server or Array Manager are allowed full privilege over the Console.



4. To add users or groups to the list, click **Add** then enter the names of users or groups. You can select groups or users clicking **browse**. Each group or user you add is given full permissions by default.
5. To delete a user or group from the list, select it and click **Remove**.

6. To change permissions for a group or user, highlight the group or user name in the top pane. The lower pane shows the current permissions for this user. Set permissions for this user by selecting the appropriate boxes.
7. Repeat Step 6 for each group or user.
8. To save the changes, click **Apply** or **OK**.
9. To apply the changes, click **Commit Configuration Changes**.

## ***Configuring Default Folder Access***

You can set the default folder permissions to control user ability to view and manipulate items in most MailMarshal SMTP folders.

### **To configure default access permissions for MailMarshal SMTP folders:**

1. Open the MailMarshal SMTP Configurator.
2. In the left pane, select **Folders**.
3. On the Action menu, click **Properties**.
4. This window displays a list of users and groups and shows the permissions they have over the features of MailMarshal SMTP folders.
5. To add users or groups to the list, click **Add** then enter the names of users or groups. You can select groups or users using the Browse Network Users window. Each group or user you add is given full permissions by default.
6. To delete a user or group from the list, select it and click **Remove**.
7. To change permissions for a group or user, highlight the group or user name in the top pane. The lower pane shows the current permissions for this user. Set permissions for this user by selecting the appropriate boxes.
8. Repeat Step 7 for each group or user.
9. To save the changes, click **Apply** or **OK**.

## ***Configuring Access for a Specific Folder***

Set the permissions on a particular folder to control user ability to view and manipulate items in that folder. Permissions on a specific folder override the default folder permissions.

**To configure access permissions for a specific MailMarshal SMTP folder:**

1. Open the MailMarshal SMTP Configurator.
2. In the left pane, expand **Folders**.
3. In the right pane, click a specific folder. Then click the **Properties** icon in the toolbar or the taskpad header.
4. Select the Security tab of the folder properties. This tab displays a list of users and groups with permission over the features of the folder.
5. To override the default security settings, select the check box **Override default folder security**.
6. To add users or groups to the list, click **Add** then enter the names of users or groups. You can select groups or users using the Browse Network Users window. Each group or user you add is given full permissions by default.
7. To delete a user or group from the list, select it and click **Remove**.
8. To change permissions for a group or user, highlight the group or user name in the top pane. The lower pane shows the current permissions for this user. Set permissions for this user by selecting the appropriate boxes.
9. Repeat Step 8 for each group or user.

10. To save the changes, click **Apply** or **OK**.

11. To apply the changes, click the **Commit** button in the toolbar.



**Note:** Setting access permissions for a folder in MailMarshal SMTP does not affect the Windows file permissions for the folder or items in it. To limit access through Windows, set the Windows access permissions for the MailMarshal SMTP Quarantine folder and all items in that folder on each MailMarshal SMTP email processing server.

To ensure that only the users with MailMarshal SMTP permissions can access these items, give full control of the Quarantine folder to the LocalSystem account or other account used by the MailMarshal SMTP services, and deny access to all other accounts.

## Viewing Event History

Each component of MailMarshal SMTP writes messages to the Windows application log. Each event type is given a unique Event ID number. You can review these events using the Console. You can also use these events to trigger automatic actions such as pager notifications, service restarts, or popup notifications via third-party products.

To review the event logs, in the Console select **Event History** in the left pane. When this node is selected, the right pane shows a filtered view of the Windows event logs for MailMarshal SMTP on the array manager and all email processing servers in the installation.



**Note:** You can view information about a specific email processing server by expanding its entry under **Servers** and selecting the sub-item **Event History**.

MailMarshal SMTP provides several pre-configured filters you can use to limit the events being displayed.

You can also customize a filter, or search for a specific event.



**Note:** In the taskpad view, all event log controls and information are shown in the right pane of the Console. In the standard view, only the list of events is shown. To access controls while in the standard view, right-click the Event Log node in the Console tree. To change view, right-click the Event Log node and choose **View**.



You can click any event listed (standard view: double-click) to see the full details.

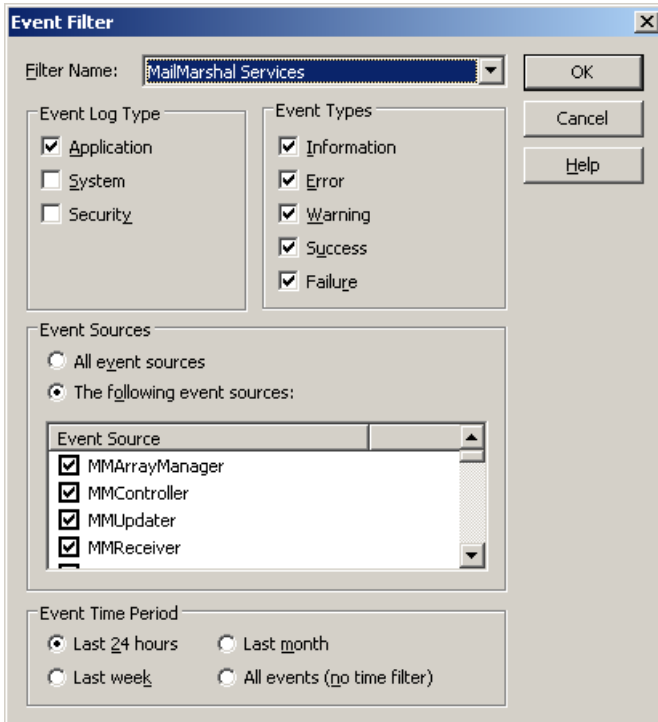
For more information, see Help.

## **Finding Events**

The MailMarshal SMTP Event Log view allows you to filter the records you retrieve, or search for specific records.

## Event Log Filter

This dialog allows you to modify the parameters of the MailMarshal SMTP event log view.



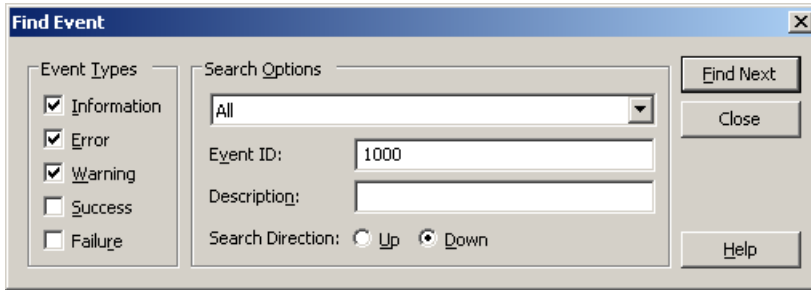
Changes you make are not saved permanently.

Enter parameters, then click **OK** to apply the filter, or **Cancel** to return to the main view.

For more information, see Help.

## Event Log Search

This dialog allows you to search for specific events in the MailMarshal SMTP event log (Taskpad view only).



Enter parameters, then click **Find Next** to find the next matching item, or **Close** to return to the main view.

For more information, see Help.

## Viewing News From M86 Security

MailMarshal SMTP Console provides access to support news and other information from M86 Security. To access this information, select **Support** in the left pane of the Console.

The Console displays the MailMarshal SMTP support page from the M86 Security website. This page gives you quick access to support resources.

The Console also provides the latest information using RSS news feeds. The Product Updates and M86 Security Labs Alerts (threat information) feeds are always enabled. New important items display in an alert window when you open the Console. You can subscribe to additional feeds and adjust settings using the Console user preferences window (click **Tools > Preferences**). For more information, see Help.



**Note:** News and alerts are retrieved from the M86 Security website, using the Internet Explorer proxy settings for the logged on user at the workstation where the Console is running.

## USING WINDOWS TOOLS

MailMarshal SMTP provides information in a standard format through the Windows event log and performance monitor.

### Event Log

Each component of MailMarshal SMTP writes messages to the Windows application log. Each event type is given a unique Event ID number. You can review these events using the Event Viewer. You can also use these events to trigger automatic actions such as pager notifications, service restarts, or popup notifications via third-party products. To open a custom view of the Event Log, use the Event History item in the Console. You can also use the Windows event viewer by selecting **Open Event Viewer** from the Tools menu of the Configurator.

### Performance Monitor

Each core service of MailMarshal SMTP (the Engine, Receiver, and Sender) makes several counters available to the Windows Performance Monitor. To open the Performance Monitor while using the MailMarshal SMTP Configurator, select **Open Performance Monitor** from the Tools menu.

Please see the documentation for Performance Monitor to learn more about its capabilities, which include remote monitoring

## USING MAILMARSHAL SMTP TEXT LOGS

Each MailMarshal SMTP service creates its own daily log files. These files provide a detailed record of routine processing and any problems encountered. The most recent information is at the end of the log file. The files are located in the Logging folder. By default, this folder is within the MailMarshal SMTP installation folder. MailMarshal SMTP keeps 6 days of log files by default.

When a MailMarshal SMTP rule is set up to move or copy a message to a folder, it can also copy the portion of the log file that relates to the message. You can see these message logs when you view a message in the Console. For more information, see “Working With Email Messages” on page 236.



---

## Chapter 9

# Managing MailMarshal SMTP Configuration

This chapter discusses a number of configuration options and tasks that maintain and customize your MailMarshal SMTP environment.

## MANAGING YOUR MAILMARSHAL SMTP LICENSES

MailMarshal requires a valid license key in order to process email. When you install MailMarshal, the installation process inserts a temporary license key valid for 30 days from the time of installation. Contact a M86 Security Sales Representative to purchase the product and receive a full license key, or to request an extended trial. If you have received a valid permanent key, you can enter it at any time using the procedure given in “Entering a License Key” on page 259.

Install licenses at the array level. The licenses apply to all MailMarshal SMTP installations in an array.

Permanent MailMarshal license keys are keyed to the list of local domains you enter. If you change the list of local domains the key will become invalid, MailMarshal will notify you and generate a temporary key valid for 14 days. You should immediately request a new key using the procedure given later in this section.



**Notes:** *MailMarshal is licensed according to the number of email users in your organization. If you exceed the licensed number MailMarshal will inform you. This event will not have any effect on email processing.*

- *If you change local domains frequently, M86 Security can provide a key based on your computer or domain SID. This key will not become invalid when you change local domains.*

## Reviewing Installed Licenses

Use the Configurator to view the details of all installed license keys, including the expiry date, number of users, and any optional features licensed.

### To view details of the currently installed license:

1. Select **MailMarshal Properties** from the Tools menu. Select **License** from the left pane.
2. You can select how MailMarshal will behave if the license expires or becomes invalid.
  - If you select **Pass through all email**, MailMarshal will function as an email relay. MailMarshal will pass messages on to their destinations without applying any engine based policy
  - If you select **Halt all processing and hold all email**, MailMarshal will continue to accept messages so long as there is available disk space for the incoming queue. MailMarshal will not deliver any messages until you enter a valid license or change this option to pass through all email.
3. To apply the selection, click **OK** then commit the configuration.



## Requesting a New License Key

To include all information required for M86 Security to generate an appropriate key, request the key through the Configurator.

**To request a new license key:**

1. On the Tools menu, select **View License Details**.
2. Click **Request Key**.
3. Complete the required information on the Request License Key window. MailMarshal will append the information required to generate a unique key.
4. To email the request to M86 Security, click **Send Request**.



***Note:** When you click Send Request, MailMarshal also places the additional request information on the Clipboard. You can paste this information to any application if you need to send a request manually.*

## Entering a License Key

When you receive a key from M86 Security, use the Configurator to enter it and verify its validity.

**To enter a license key:**

1. Select **View License Details** from the Tools menu.
2. Click **Enter Key**.
3. Enter the key, and select how MailMarshal will behave if the license expires or becomes invalid.
4. Click **OK**. MailMarshal will report the validity of the key you entered.

5. **If your key expired**, MailMarshal SMTP might have stopped the Engine service. Verify that all services are running on all email processing servers by completing the following steps:
  - a. In the left pane of the Configurator, select **Server and Array Configuration**.
  - b. MailMarshal SMTP displays all servers in the array. Select a server and click **Server Properties**.
  - c. **If a MailMarshal SMTP service is stopped**, click **Start**.
  - d. Repeat step c to verify each server service in your array is started.

## BACKING UP AND RESTORING THE CONFIGURATION

You should back up your MailMarshal SMTP configuration at the following times:

- Before and after you make substantial MailMarshal SMTP configuration changes using the Configurator.
- Before applying an upgrade.

You can restore the configuration when you want to make the following changes:

- Create a new Array Manager server.
- Return to a previous version of your email policy.

In addition to the following backup and restore procedures, you can back up and restore the configuration using a command line prompt. For more information see “Using the Configuration Export Tool” on page 300.

You can import your user and group information using the MailMarshal SMTP Configurator. For more information see, “Configuring User Groups” on page 179.

You can also import user group information using a command line prompt. For more information see “Using the Group File Import Tool” on page 298.

For more information about backing up the \Quarantine folders and the MailMarshal SMTP database, see the M86 Security Knowledge Base.

## Backing Up the Configuration

Backing up the MailMarshal SMTP configuration includes running Backup in the Configurator and backing up the following additional files:

Computer	Folder	Files
Array Manager	Folder you specify during Backup operation (by default, <i>installpath</i> )	<i>backupconfig.xml</i> (for example, Backup20050607.xml)
Array Manager	<i>InstallPath</i>	filetype.cfg
Array Manager (optional)	<i>InstallPath</i> \Logging	*.log
Email processing servers	<i>InstallPath</i> \Quarantine and <i>InstallPath</i> \Quarantine \ValidFingerprints	*.*

Where *InstallPath* indicates the location where you installed the product. The default install path is \Program Files\Marshal\Mai I Marshal .



**Note:** The backup does not include the members of groups imported from directory connectors.

**To back up the MailMarshal SMTP configuration:**

1. On the Array Manager computer, run the MailMarshal SMTP Configurator from the MailMarshal program group.
2. On the Tools menu, select **MailMarshal Properties**.
3. Select **General** from the left pane and click **Backup**.
4. Specify the name of the backup file you want to create. For example, specify `\InstallPath\Backup20050609.xml`.
5. Make a note of the backup filename and location.
6. Click **OK**.
7. **If you have created file type rules**, back up the filetype.cfg file in the `\InstallPath` folder.
8. Make a note of each MailMarshal SMTP email processing server computer name.
9. On each MailMarshal SMTP email processing server computer, back up the `\InstallPath\Quarantine` and `\InstallPath\Quarantine\ValidFingerPrints` folders by following the instructions in Knowledge Base article Q10220.
10. **If you are using a MailMarshal SMTP array**, repeat Step 10 on every email processing server in the array.
11. Make a note of the MailMarshal SMTP database computer name.
12. On the database computer, back up the MailMarshal SMTP database by following the instructions in Knowledge Base article Q10221.

## Restoring the Configuration

Restoring the MailMarshal SMTP configuration requires a number of steps. You can restore the configuration if you are creating a new Array Manager server, or if you want to return to a previous version of your email policy.



**Note:** The restored data does not include the members of groups imported through directory connectors. **To retrieve the group members:** After restoring the configuration, in the left pane of the Configurator right-click **User Groups** and select **Reload User Groups**.

### To restore your MailMarshal SMTP configuration:

1. On the Array Manager computer, run the MailMarshal SMTP Configurator from the MailMarshal program group.
2. On the Tools menu, click **MailMarshal Properties**.
3. Select **General** from the left pane and click **Restore**.
4. Enter or browse to the backup configuration file. For example, browse to `\\InstallPath\Backup20050609.xml`.
5. Click **OK**.
6. **If MailMarshal SMTP prompts you**, click **OK** to commit configuration changes.
7. To restore custom file type definitions, copy the back up `filetype.cfg` file to the `\\InstallPath` folder on the Array Manager computer.
8. To repopulate users in LDAP and Active Directory user groups with current members:
  - a. In the left pane of the Configurator, expand **MailMarshal Configurator > Policy Elements** and select **User Groups**.
  - b. On the Action menu, click **Reload User Groups**.
9. To retrieve the latest Spam Censor definition file, `spamfilter.xml`:

- a. On the Tools menu, select **MailMarshal Properties**.
  - b. Select **Automatic Updates** in the **left pane** and click **Check for Updates Now**.
  - c. When the update is complete, click **OK** and then click **Commit Configuration**.
10. On each MailMarshal SMTP email processing server computer, restore the `\InstallPath\Quarantine` and `\InstallPath\Quarantine\ValidFingerPrints` folders by following the instructions in Knowledge Base article Q10220.
  11. *If you are using a MailMarshal SMTP array*, repeat Step 13 on every email processing server in the array.
  12. On the database computer, restore the MailMarshal SMTP database from the backup copy. For more information about restoring a database file, see the Microsoft SQL Server or SQL Express documentation.
  13. To connect to a new or existing MailMarshal SMTP database, connect to the database using the MailMarshal SMTP Server Tool. For more information, see “Joining a Node to an Array” on page 285 and “Working with Array Communications” on page 294.

## CONFIGURING LOCAL DOMAINS

You configure a list of local email domains when you install MailMarshal SMTP. You may need to update this configuration if you change internal email servers, or if you add more Internet domains.



**Note:** *The list of local domains configured in MailMarshal SMTP should always match the DNS MX records that direct email from the Internet to MailMarshal SMTP.*

You can specify delivery options for local domains as part of a Route Table. Delivery options include relay to an internal email server (known as a **relay domain** in earlier versions of MailMarshal SMTP), or POP3 delivery by MailMarshal SMTP (known as a **POP3 domain** in earlier versions of MailMarshal SMTP).



**Note:** *Appliance installations do not support POP3 domains.*

If you are using an array of MailMarshal SMTP email processing servers, you can choose to set different delivery routes on each email processing server.

To view the list of configured Local Domains, in the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration > Local Domains**.

## Changing Local Domains Information

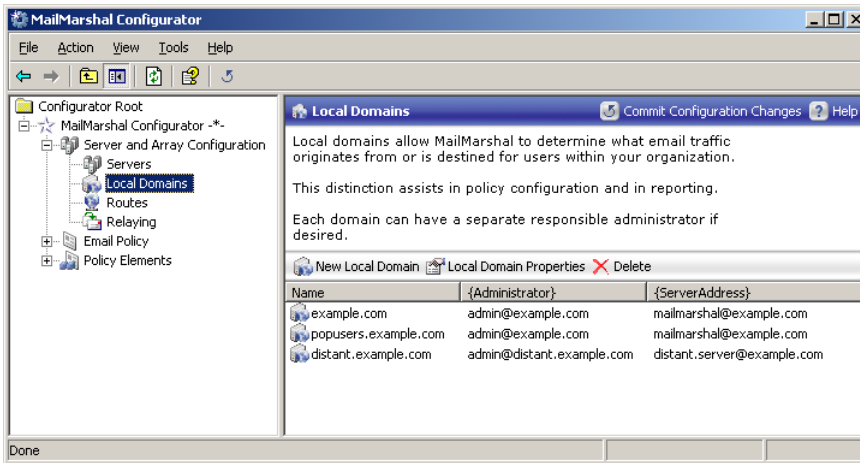
You can change the list of domains MailMarshal SMTP recognizes as local.



**Note:** *To change delivery locations for Local Domains, see “Configuring Routes” on page 267.*

### To change the list of local domains:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration > Local Domains**.
2. The Local Domains window displays a list of the local domains, and the administrative addresses associated with each domain.



### 3. Select the action you want to perform:

- To create a new local domain listing, click **New Local Domain**.
- To edit an existing local domain listing, highlight it and then click **Local Domain Properties**.
- To delete an existing local domain listing, highlight it and then click **Delete**.

For details of the fields on the Local Domain windows, see Help for each window.



# CONFIGURING ROUTES

MailMarshal SMTP uses Routing Tables to determine where and how to deliver email messages. When you install MailMarshal SMTP, the Configuration Wizard creates a basic Routing Table with a single entry for Local Domain email and a single entry for outgoing email.

You can add entries to the Routing Table to support a number of routing scenarios, such as:

- **Load Balancing:** Multiple entries for the same destinations, used alternately.
- **Fallback Delivery:** Additional entries for the same destination, used only when delivery fails.
- **Custom delivery** for a domain: Additional destination entries, used to deliver email addressed to specific local or remote domains through specific servers.
- **SMTP Authentication** for a route: Authenticated connection to the server that MailMarshal SMTP uses to deliver messages for the route.

A routing destination can be defined by an IP address, a host name, MailMarshal SMTP POP3, or DNS MX resolution.

You can create additional routing tables to support different routing from each processing server in a MailMarshal SMTP Array. For more information about advanced routing configuration, see M86 Security Knowledge Base article Q11914.

To view the list of configured Routing Tables, in the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration > Routes**.

## Editing Routing Table Information

You can add new routing tables, and edit existing tables.

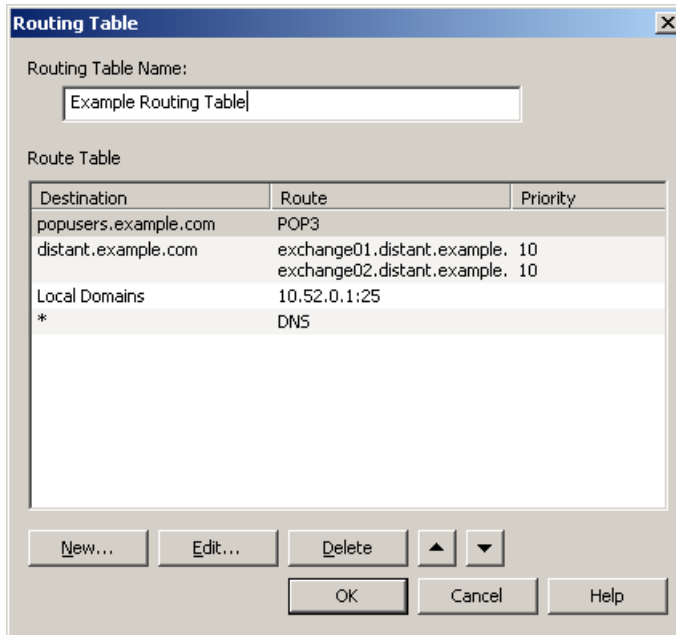


**Note:** To change the tables used for delivery, see “Configuring Delivery Options” on page 275.

### To change the routing tables:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration > Routes**.
2. The Routes window displays a list of the routing tables.
3. *If you want to create a new routing table*, click **New Routing Table**.

4. *If you want to edit an existing routing table*, highlight it and then click **Routing Table Properties**.



## 5. The Routing Table listing shows a list of destinations.



**Note:** A destination can be “Local Domains,” “Default Route” (normally used for delivery of outgoing messages and shown as \*), or a specific domain.

- Each destination entry can be associated with one or more routes.
- Each route has a priority expressed as a number. Lower numbered routes to a destination will be used first.
- A route can support SMTP authentication (indicated in the table as [AUTH])

a. To create a new destination entry, click **New**.

b. To associate a new route with a destination entry, on the Domain Routing window, click **New**.

- If you want MailMarshal SMTP to deliver outbound email directly, set a destination of **Resolve using DNS** for the Default Route.
- If you want to send all outbound email to a firewall, or to a relay server at your ISP, add a route using the IP address or host name. When you send outbound email to another server, that server is responsible for final delivery.
- If you want to create load-balanced delivery for a destination, add multiple routes with the same priority. (Set priority on the Advanced tab of the Route Entry window.)
- If you want to create a primary and fallback delivery option for a destination, set a lower number (higher priority) for the primary route. (Set priority on the Advanced tab of the Route Entry window.)

- To adjust the order of destination entries, use the arrow buttons on the route table window.

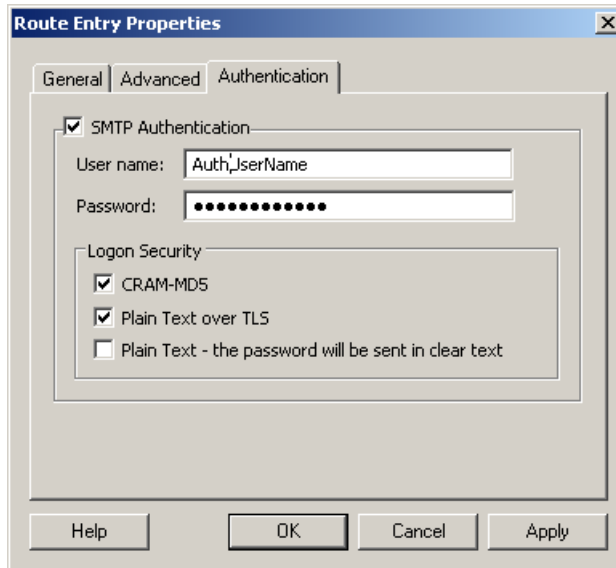


**Note:** *If you have route table entries for specific domains, you may need to adjust the order of destinations to ensure proper handling. For example, consider the following routing table:*

popusers. exampl e. com	POP3
*. exampl e. com	exchange01. exampl e. com: 25
Local Domai ns	10. 52. 0. 1: 25
* (defaul t)	DNS

*In this order, email addressed to popusers. exampl e. com is delivered to POP3 mailboxes on the MailMarshal SMTP server, but email addressed to any other subdomain in exampl e. com is forwarded to the relay server exchange01. di stant. exampl e. com on port 25. If you change the sequence and put \*. exampl e. com first in the list, email addressed to popusers. exampl e. com is relayed before it can be delivered to the POP3 mailboxes, because pop. exampl e. com also matches \*. exampl e. com.*

- If you want to use authenticated SMTP connections, select from the options on the Authentication tab of the Route Entry window. Determine the appropriate username, password, and supported methods from the administrator of the remote server. MailMarshal SMTP supports the CRAM-MD5, LOGIN, and PLAIN options for SMTP authentication. Additionally, authentication can be within a TLS session. For more information about the supported methods and behavior of this feature, see Help.



**6. If you want to delete an existing routing table, highlight it and then click Delete.**

For additional details of the routing table options, see Help for each window.

# CONFIGURING RELAYING

MailMarshal SMTP uses Relay Tables to determine which computers are allowed to send outgoing email through the MailMarshal SMTP installation. When you install MailMarshal SMTP, the Configuration Wizard creates a basic Relay Table that typically allows outgoing email from your Local Domain email server.

You can add entries to the Relay Table to support relaying from additional locations inside or outside your local network. Relaying is only allowed by explicit entries in the table.



**Note:** *Earlier versions of MailMarshal SMTP always allow relaying from the Local Domain server without requiring an explicit entry in anti-relaying settings. MailMarshal 6.4 requires entries in Relay Tables.*

You can create additional relay tables to support different relaying permissions from each processing server in a MailMarshal SMTP Array. For more information about advanced routing configuration, see M86 Security Knowledge Base article Q11914.

To view the list of configured Relaying Tables, in the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration > Relaying**.

## Editing Relay Table Information

You can add new relay tables, and edit existing tables.

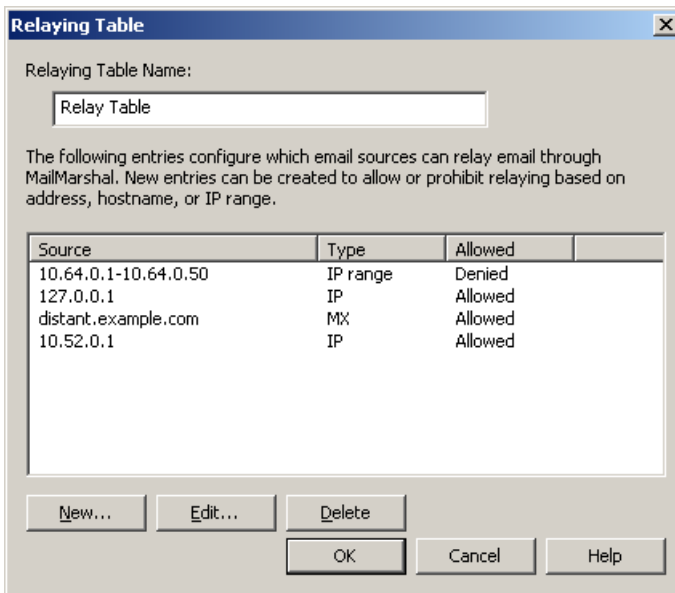


**Note:** *To change the tables used to control relaying on each processing server, see “Configuring Delivery Options” on page 275.*

### To change the relay tables:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration > Relaying**.
2. The Relaying window displays a list of the relaying tables.
3. Select the action you want to perform:
  - To create a new relaying table, click **New Relaying Table**.
  - To edit an existing relaying table, highlight it and then click **Relaying Table Properties**.
  - To delete an existing relaying table, highlight it and then click **Delete**.

Each relay table can include multiple entries that define the servers allowed and denied relaying permission.





For details of the relaying table options, see Help for each window.

## CONFIGURING DELIVERY OPTIONS

MailMarshal SMTP distinguishes between “inbound” and “outbound” email.

Inbound email is email delivered to your organization. MailMarshal SMTP determines how to deliver this email based on your local domains. For more information about local domains see “Configuring Local Domains” on page 264.

Outbound email is email delivered to locations outside your local domains. MailMarshal SMTP can deliver this email directly using DNS lookups, or by forwarding all email to a relay host.

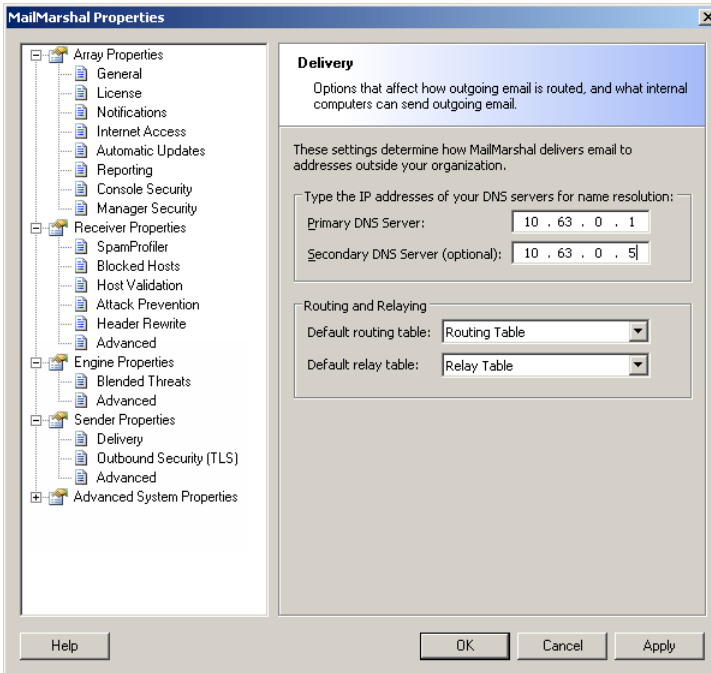
You configure basic delivery options using the Configuration Wizard when you install MailMarshal SMTP. You can make changes later if required.

## Configuring Default Delivery Options

You can make changes to default delivery options for the entire installation using MailMarshal Properties.

**To configure delivery options:**

1. Select **MailMarshal Properties** from the Tools menu and select **Delivery** from the left pane.



2. Enter a primary DNS (Domain Name Server) address used by your organization. Optionally enter a secondary DNS address. These servers should be in the local network if possible, but in any case no further away than your ISP. They must be able to resolve domain names outside your organization.



**Notes:** MailMarshal SMTP does not use the DNS servers configured in Windows networking.

- If MailMarshal SMTP must perform DNS lookups through a firewall, the firewall must permit both TCP and UDP based lookups.
3. Select a Routing Table that defines how MailMarshal SMTP should deliver email messages. For more information about Routing Tables, see “Configuring Routes” on page 267.
  4. Select a Relaying Table that defines the servers MailMarshal SMTP will allow to send outgoing mail. For more information about Routing Tables, see “Configuring Relaying” on page 273.
  5. To complete the changes, click **OK** on the MailMarshal Properties window and commit the configuration.

## Configuring Delivery Options For A Specific Server

If you are using an array of MailMarshal SMTP servers, you can choose to set delivery options for each server.

### To set delivery options for a specific server:

1. Select **Servers** by expanding **Server and Array Configuration** in the left pane.
2. Highlight a server on the Action menu and click **Properties**.
3. On the MailMarshal Properties window select **Delivery**.

4. In the right pane, select **Customize the Delivery Settings**.
5. Change the entries as desired. For details of the fields and settings, see “Configuring Default Delivery Options” on page 276.

## SETTING UP ACCOUNTS

MailMarshal SMTP accounts consist of a user name and password. You can use accounts for two purposes:

- To authenticate user connections using a receiver rule. For more information, see “Where sender has authenticated” on page 157.



**Note:** *If you use this feature to allow one or more accounts to relay email, consider the following best practices:*

- *Ensure that these accounts have strong passwords. If an account password is guessed by a malicious person, MailMarshal SMTP could become an open relay. Change the passwords periodically.*
  - *Use accounts that are only used for this purpose, and not Windows accounts with other permissions. Password transmission during authentication is not strongly secured.*
- To specify users for the MailMarshal SMTP POP3 server. If you will be using accounts for POP3 delivery, set up a default routing table with POP3 routing for all required domains before creating accounts. For more information about POP3 domains, see “Editing Routing Table Information” on page 268.



**Note:** *The MailMarshal SMTP POP3 server is not designed to be used in an installation with more than one email processing server.*

## Creating Accounts

Create accounts using the MailMarshal SMTP Configurator.

### To create accounts:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Policy Elements > Accounts**.
2. On the Action menu, choose **New Account**.
3. Enter the details for the user name and authentication information in the New Account window.
4. MailMarshal SMTP will automatically enter an appropriate SMTP alias for email delivery to this account's mailbox, based on the default Routing Table. If more than one POP3 domain is configured, MailMarshal SMTP will enter an alias for each domain.



**Notes:** *If the routing table includes POP3 delivery for "Local Domains," MailMarshal SMTP will enter the special value "Local Domains." This entry ensures that email directed to the account name at any local domain will be correctly delivered. You should not edit this value.*

- *If you want to use the account only for authentication, type none.*
- *Appliance installations do not require or permit SMTP Aliases. Aliases are only used for POP3 delivery, which is not supported in these installations.*

5. Make any desired changes to the list of SMTP aliases.
6. ***If you want email for other SMTP addresses to be delivered to this account's mailbox***, enter the complete addresses manually. Enter one address per line. Use the Enter key to move between lines. Only use domain names for which MailMarshal SMTP is functioning as a POP3 local domain server.



**Note:** *If you enter the same SMTP alias in more than one POP3 account, messages directed to that alias will be delivered to all of the mailboxes*

7. If the password fields are blank, MailMarshal SMTP will use Windows authentication to determine access for this account. In this case, ensure that the account name matches the name of a valid Windows user account permitting access to files on the MailMarshal SMTP server computer.
8. To add the account, click **Add**.
9. When you have added all accounts, click **Close**.
10. Click **Commit Configuration Changes**.

## Editing Existing Accounts

Edit an account to change the password or email addresses associated with the account.

### To edit an existing account:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Policy Elements > Accounts**.
2. Double-click the account you want to edit.
3. Change the password and aliases as required.
4. Click **OK**.

## Deleting Accounts

Delete accounts that are no longer required. If you delete an account used for email delivery, you should also delete the delivery folder from the MailMarshal SMTP sending queue directory.

### To delete an account:

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Policy Elements > Accounts**.
2. Select the account you want to delete.

3. Click the **Delete** icon in the toolbar.
4. Using Windows Explorer, navigate to  
C: \Program Files\Marshal \Mail Marshal \Queues\Sending\<account\_file>  
.
5. Back up the contents of the account file that you deleted.

Delete the account file.

## CONFIGURING EMAIL BATCHING

MailMarshal SMTP supports batch receipt and sending of email messages where you do not want to have an on-demand connection to the downstream email server. Mail batching is implemented through the `MMGetMail.exe` helper application. You can use this application in batch files or custom scripting. For more information about `MMGetMail`, see M86 Security Knowledge Base article Q10285.



**Notes:** *The integrated Mail Batching and Dial-Up Networking functions that were available in earlier versions of MailMarshal SMTP have been discontinued.*

## CONFIGURING MANAGER SECURITY

You can control access to the MailMarshal SMTP Array Manager. To perform some tasks a user must have an account that the Manager can validate. As of this writing the only permission you can control is permission to join an email processing server to an array.

**To configure access to Array Manager features:**

1. Open the MailMarshal SMTP Configurator.
2. On the Tools menu, select **MailMarshal Properties**.

3. From the left pane select **Manager Security**. A list of users and groups with permission over the manager features is displayed. By default all members of the Windows Administrators group on the MailMarshal SMTP server or Array Manager are allowed full permissions over all items that are secured through on the window.
4. To add users or groups to the list, click **Add** then select groups or users using the Browse Network Users window. Each group or user you add is given full permissions by default.
5. To delete a user or group from the list, select it and click **Remove**.
6. To change permissions for a group or user, highlight the group or user name in the top pane. The lower pane shows the current permissions for this user. Set permissions for this user by selecting the appropriate boxes.
7. Repeat Step 6 for each group or user.
8. To save the changes, click **Apply** or **OK**.
9. To apply the changes, commit the configuration.

## MANAGING ARRAY NODES

A MailMarshal SMTP installation consists of an Array Manager and one or more email processing servers, also known as array nodes.

### Managing Node Services

You can view the status of the MailMarshal SMTP services on each email processing node, and stop or restart the services, from the MailMarshal SMTP Configurator.

To see an overview of the status of services on each node, in the left pane of the Configurator click **MailMarshal Properties**.



**To see details of the status of services on a particular node, and to stop or restart the services:**

1. In the left pane of the Configurator expand **Server and Array Configuration**. Highlight **Servers**. The list shows all servers and a summary of the state of each server. (For more details about the information listed, see Help.)
2. In the right pane select the server you want and click **Properties**.
3. Select **General** from the left pane to see the Services listing and to see the status of each service installed on the node.
4. To stop one or more services, select them in the list then click **Stop**.
5. To start one or more services, select them in the list then click **Start**.
6. To restart all services, click **Restart all**.



**Note:** *If you stop services from this window, they will remain stopped until you start them. Committing the configuration will not start the services.*

## Adding and Deleting Nodes

You can add email processing servers (nodes) to a running MailMarshal SMTP installation to add capacity or redundancy. You can also delete existing nodes from an installation.

### ***Adding a Node***

You can add a node at any time without affecting other nodes. After adding the node, adjust email routing so that the new node shares in email processing. Contact your internet service provider or DNS administrator, as necessary.



**Note:** *Adding a node does not create automatic load balancing.*

**To add a node to a MailMarshal SMTP installation:**

1. Log on to the new server using an account that you have granted the permission **Join Array**.
2. Install MailMarshal SMTP.
3. During installation, select the option “I want to join an existing array” and enter the name of the existing Array Manager.

For more information, see “Installing MailMarshal SMTP as an Array” on page 48.

***Deleting a Node***

You should delete a node to cleanly remove it from the MailMarshal SMTP array. Before deleting a node, adjust email routing so that the node to be deleted does not process any email. Contact your internet service provider or DNS administrator, as necessary.

**To delete a node from a MailMarshal SMTP installation:**

1. Stop MailMarshal SMTP services on the node using the MailMarshal SMTP Configurator.
2. If you want to preserve messages from quarantine folders stored on the node, back up the Quarantine folder in the MailMarshal SMTP installation folder on the node.
3. Uninstall MailMarshal SMTP on the node server using the Add/Remove Programs application in Control Panel.

4. During the un-installation process, MailMarshal SMTP will attempt to remove the node records from the array installation. If the logged in user does not have the “can join servers to array” permission, MailMarshal SMTP will ask for an alternate credential. If you do not remember the credential, you can still perform the un-install. In this case, remove the node records later using the Configurator.
5. In the Configurator, an un-installed node will show a status of “not active.” You can highlight the node and click the delete icon in the toolbar.

## Joining a Node to an Array

You can join an email processing server (node) to a MailMarshal SMTP array. After joining the array, the node will retrieve policy configuration from the Array Manager.

### To join an existing node to a MailMarshal SMTP installation:

1. Log on to the node server.
2. Run the MailMarshal SMTP Server Tool from the MailMarshal program group.
3. On the Node > Array page, enter the local port, and the port and server name for the Array Manager. Select **Join Array**, and then click **Apply**. Enter the credentials of an account that has the permission **Join Array** (granted in the Configurator).

## Customizing Settings for Nodes

Since the purpose of a MailMarshal SMTP array is to replicate configuration over a number of processing servers, most settings will be the same for all nodes. You can configure the following settings for each node:

### Server name and general information

For each email processing server, you can view and change the server name and the description and location notes.



**Note:** Only change the server name here if you have changed the computer name of the email processing server.

### Delivery information

For each email server in an array, you can specify DNS servers, and the relay and routing tables to use. One use of this override would be to allow geographically separated MailMarshal SMTP servers to deliver inbound email to different internal email servers.

### Internet Access information

For each email server in an array, you can specify proxy settings (or direct access) that will allow the server to retrieve SpamProfiler and Blended Threats Module updates over the Internet.

### Inbound TLS information

For each email server in an array, you can configure Transport Layer Security (TLS) usage including a certificate.

### Advanced server information

For each email server in an array, you can choose one or more IP addresses and ports the MailMarshal SMTP Receiver will bind to. You can specify what percentage of available threads each address:port can use. This setting allows you to reserve some Receiver capacity for specific connections (for instance to ensure that outgoing email will be accepted even if incoming volume is high).



**Note:** *By default, the Receiver binds to port 25 on all configured IP addresses. This setting allows MailMarshal SMTP to receive all email sent to each email processing server at the default SMTP location. If you customize the Receiver bindings, ensure that you add a setting for each configured address.*

You can specify a host name, which may be required if this information is not entered in the Windows networking properties. You can also select whether the email processing server should be preferred by the Array Manager as a host to be used in sending notifications.

### To customize settings for a particular node:

1. In the left pane of the Configurator, expand **Server and Array Configuration**.
2. Select **Servers**, and then in the right pane double click the node you wish to configure.
3. To navigate through the available settings for the node, select items in the left pane of the window. For detailed information about the settings, click **Help**.
4. When you have configured any changes required, click **OK**.

## Managing Appliance Nodes

In Appliance installations, you join a node to an array using the node configuration wizard and node window on the appliance web interface. For details see the Help on the appliance web interface.

The following additional item is available in the node properties within the Configurator:

### **McAfee Updates information**

This tab displays details of the last update and current DAT file version for McAfee for Marshal on the node. You can force an immediate check by clicking **Update**.

## **UNDERSTANDING SECURE EMAIL COMMUNICATIONS**

MailMarshal SMTP allows you to secure outgoing and incoming email using transport layer security (TLS), an implementation of secure sockets layer (SSL).

TLS secures the privacy of the communications channel and provides one-way authentication. TLS is generally used to provide a secure (encrypted) transport over which email communications including the headers, body and attachments are delivered. TLS is generally *not* used to guarantee server authenticity.

Use TLS when you want to secure your organization's email from being read by unauthorized users inside or outside of your organization. Secure email may be required if your organization sends or receives mail containing information that is protected under laws, such as the US Health Insurance Portability and Accountability Act (HIPAA).

TLS uses public-private key pair encryption on each MailMarshal SMTP server to secure an email communications channel and to authenticate itself to clients.



**Notes:** *TLS slows your email operations to a limited degree.*

- *TLS works only when ESMTP (EHLO extensions) is enabled. (This is the default setting.) TLS does not work with HELO.*

# SECURING EMAIL COMMUNICATIONS

You can use MailMarshal SMTP to secure incoming and outgoing email communications. MailMarshal SMTP allows you to decide where and under what conditions you want to use TLS. Setting up TLS involves 3 tasks:

1. Creating or importing a TLS Certificate
2. Enabling TLS for mail incoming to MailMarshal
3. Enabling TLS for mail outbound from MailMarshal

**Note:** For more information about configuring TLS, see M86 Security Knowledge Base article Q11636

## Working with Certificates

Each MailMarshal SMTP server using TLS makes its secure status public using a certificate. MailMarshal SMTP stores TLS Certificates on each server. For each MailMarshal SMTP server with which you want to use TLS, you must generate or obtain an authentication certificate. To perform these tasks, use the TLS Certificate Wizard.

Certificates have expiration dates. Starting two weeks before a certificate expires, MailMarshal SMTP sends a daily renewal reminder email to the MailMarshal SMTP administrator.

The TLS Certificate Wizard allows you to perform the following tasks:

- Generate a Certificate Signing Request (CSR) that you submit to a third-party certificate authority
- Import X.509 and PKCS#7 key-certificate backup files supplied by a certificate authority
- Generate self-signed certificates
- Save server-specific key-certificate pairs as PKCS#12 files
- Import PKCS#12 files

**To create or manage certificates:**

1. In the left pane of the Configurator, expand **Configurator Root > MailMarshal Configurator > Server and Array Configuration**.
2. In the right pane, select the hostname of the MailMarshal SMTP server for which you want to configure TLS.
3. On the taskpad menu, click **Server Properties**.
4. Click **Inbound Security (TLS)**.
5. Click **TLS Certificate Wizard**.
6. Complete the wizard, by entering the required information to complete the certificate task you are performing. For more information about the fields on a window, click **Help**.
7. Click **OK**.

## Securing Inbound Communications

Using TLS is optional for incoming email. You control when and how MailMarshal SMTP uses TLS for inbound connections.

MailMarshal SMTP allows you to control incoming email TLS configuration on each email processing server in an array. You cannot apply a single configuration across an array. Repeat the following task for each email processing server.

**To enable TLS for inbound connections on a MailMarshal SMTP email processing server:**

1. In the left pane of the Configurator, expand **Server and Array Configuration**.
2. In the right pane, select **Servers** and then select the name of the email processing server for which you want to configure TLS.



3. On the taskpad menu, click **Server Properties**.
4. Select **Inbound Security (TLS)**.
5. Specify the appropriate values. For more information about the options, click **Help**.



**Note:** The **Enable TLS** option is available only when a valid certificate is installed on the server.

6. Click **OK**.

When a message is received with TLS, the Received: header line is marked with the version of TLS used. For instance:

```
Received: from client03 (Not Veri fi ed[127.0.0.1]) by vm-exampl e03 wi th  
Mai l Marshal (v6, 2, 0, 2977) (usi ng TLS: SSLv23).
```

## Securing Outbound Communications

Using TLS is optional for outgoing email. You control when and how MailMarshal SMTP uses TLS for outbound connections.

MailMarshal SMTP applies the TLS configuration for outbound email across all email processing servers in the array.

### To enable TLS for outbound email:

1. In the Configurator, click **MailMarshal Properties** on the **Tools** menu.
2. Select **Outbound Security (TLS)** from the left pane.
3. Specify the appropriate values. For more information about the options, click **Help**.
4. Click **OK**.

When a message is sent using TLS, MailMarshal classifies the message as “Delivered successfully over TLS.” You can review this information in the Console and Reports.

# SETTING ANTI-VIRUS UPDATE OPTIONS

In Appliance installations of MailMarshal SMTP, this tab allows you to view the status of Anti-Virus updates and check for new updates.

# SETTING ADVANCED OPTIONS

MailMarshal SMTP allows you to configure a number of advanced settings. These settings default to values that are reasonable in the majority of cases. In specific cases you may need to change them.

## MailMarshal Properties - Advanced

These options affect delivery and processing of email. If more than one MailMarshal SMTP server is included in an array, these options affect all servers.

### **Engine Advanced options**

Allows you to set options for RTF stamping and unpacking depth.

### **Engine Blended Threats exclusions**

Allows you to maintain a list of domains (or domain wildcard patterns) that will never be submitted for Blended Threat analysis.

### **Receiver Advanced options**

Allows you to set behaviors of the MailMarshal SMTP Receiver, including greeting strings, advertising of ESMTP, and other items.

### **Sender Advanced options**

Allows you to set behaviors of the MailMarshal SMTP Sender, including ESMTP sending and deadlettering options.

### **Server Threads**

Allows you to configure threading for optimal performance.

**Templates**

Allows you to override the administrative notification messages built in to MailMarshal SMTP.

**Times**

Allows you to set retry and expiration timeouts for the Receiver and Sender services.

**Commit Scheduling**

Allows you to specify times of day when configuration changes should be committed at the MailMarshal SMTP node processing servers. This functionality is designed to allow deferred commits so as to minimize impact on systems during the business day.

**To configure advanced server options:**

1. On the Tools menu of the Configurator, click **MailMarshal Properties**.
2. Navigate to the required option, found under Advanced System Properties, Engine Properties, or other Advanced items in the left pane of the window.
3. Specify the appropriate values. For more information about the options, click **Help**.
4. Click **OK**.

## Setting Node Properties - Advanced

These options affect delivery and processing of email. If more than one MailMarshal SMTP server is included in an array, these options can be set for each server.

- Receiver Binding
- Server Host Name
- Notification Delivery

For more information about these settings, see “Customizing Settings for Nodes” on page 286.

## Working with Array Communications

When MailMarshal SMTP is configured as an array of servers with an Array Manager and one or more other servers as email processing servers, the MailMarshal SMTP servers communicate over TCP/IP. By default, MailMarshal SMTP uses port 19001. If the Array Manager and email processing services are installed on the same server, by default the email processing services use port 19002.

You can configure these settings using the MailMarshal SMTP Server Tool, which is installed on each server. You must configure the settings on each server individually.



**Note:** Close the MailMarshal SMTP Configurator and Console applications while using the Server Tool.

### Changing Array Port Settings

You can change the TCP ports used by the MailMarshal SMTP services. For instance, you may want to alter the default port numbers to enhance security.

#### To change the port settings:

1. Log on to the server using an account with Administrator permissions.
2. Run the MailMarshal SMTP Server Tool from the MailMarshal SMTP Tools group in the MailMarshal program group.

3. **If the server is an email processing server** (not an Array Manager or standalone server):
  - a. On the Node > Array page, you can change the Node Port used by the services to listen for communications from the Array Manager. When you apply this change and restart the services, MailMarshal SMTP will report the change to the Array Manager.
  - b. You can also change the Array Manager port used by the services to connect to the Array Manager. This entry must match the port specified at the Array Manager.
4. **If the server is an Array Manager:** On the Array Manager > Ports page, you can change the port used by the Array Manager to accept connections from email processing servers, the Console, the Configurator, and the Web components.



**Note:** If you change this value, to restore full functionality you must also change the corresponding value in several other places. These include each email processing server and the Web components if installed. The Configurator and Console installations will prompt for a new port when they are next opened.

## **Changing the Database Location**

You can change the location of the MailMarshal SMTP database using the Server Tool on the Array Manager server. Because most configuration information is stored in the database, in general you should only use this option if you must change the Microsoft SQL Server on which the database is hosted.

When you create a new database, MailMarshal SMTP does not retain Spam Quarantine Management logs and related data.

**To change the database location:**

1. Back up the MailMarshal SMTP configuration. See “Backing Up and Restoring the Configuration” on page 260.
2. Log on to the Array Manager server using an account with Administrator permissions.
3. Run the MailMarshal SMTP Server Tool from the MailMarshal Tools group in the MailMarshal program group.
4. *If you want to move the existing database:*
  - a. Stop all MailMarshal SMTP services.
  - b. Move the database to the new location using Microsoft SQL Server tools.
5. On the Database page, enter the new SQL Server name and database name. Click **Apply**. If necessary, MailMarshal SMTP will present options to use or recreate an existing database. *If you have moved a database and selected it*, choose **Use** and click **OK**.
6. If the Array Manager also hosts a processing node, MailMarshal will offer to rejoin the node to the array. You must complete this step either now or later.
7. MailMarshal SMTP will ask to restart services. You must complete this step either now or later.
8. Restore the MailMarshal SMTP configuration. For more information, see “Backing Up and Restoring the Configuration” on page 260.
9. *If the installation is an array with additional processing nodes*, use the Server Tool on each email processing server to rejoin the servers to the array. See “Joining a Node to an Array” on page 285.

## Changing Folder Locations

You can change the default location for MailMarshal SMTP logging, quarantine, message unpacking, and message queues on each email processing server using the MailMarshal SMTP Server Tool. For more information about the how these folders are used, see “Understanding MailMarshal SMTP Folder Locations” on page 37.

### To change the locations of folders:

1. Using the MailMarshal SMTP Configurator, stop the MailMarshal SMTP services on the email processing server where you want to move folders.
2. Log on to the email processing server using an account with Administrator permissions.
3. Run the MailMarshal SMTP Server Tool from the MailMarshal Tools group in the MailMarshal program group.
4. On the Array Manager > Folders page and/or the Node > Folders page, change the locations. You can enter a full path relative to a local drive letter, or a partial path relative to the MailMarshal SMTP installation folder.
5. Click **OK**. The Server Tool will offer to copy files from the old locations. The Server tool will also offer to restart the MailMarshal SMTP services.
6. The Server Tool will not delete files from the old locations. You can safely do so using normal Windows procedures.



**Note:** You can change the location of an individual folder. For more information, see “Working with Folders” on page 215.

# USING THE GROUP FILE IMPORT TOOL

The MailMarshal SMTP Group File Import Tool is a command-line tool you can use to import information into MailMarshal SMTP user groups if your environment does not support Active Directory or LDAP.

**Warning:** *When the Group File Import tool is in use, MailMarshal SMTP temporarily bounces incoming email. Use this tool during off-peak hours.*

If your environment includes a structure that uses Active Directory or LDAP, rather than using the group file import tool, set up a Connector and allow MailMarshal SMTP to populate your User Groups from the directory. For more information, see “Configuring Connectors” on page 177 and “Configuring User Groups” on page 179.

If you want to import POP3 mailboxes for use with MailMarshal SMTP, use the POP3AcctUtil.exe utility. For more information, see Knowledge Base article Q10216.

Run the GroupFileImport.exe from the MailMarshal SMTP *InstallPath* folder. By default, the installation path is `\Program Files\Marshal\Mai l Marshal .`

## To use the group file import tool:

1. Using a text editor such as Notepad, create the input file that contains the names of the groups and user email addresses you want to import. For more information, see “Group File Import Text File Format” on page 299.
2. Log onto the Array Manager computer as a member of the local Administrators group or other user account with permissions to modify the registry.
3. Open a command window and navigate to the folder where you installed MailMarshal SMTP.



4. Type the group file import command with the options you want to specify. For more information, see “Group File Import Command Format” on page 299.
5. After the users and groups are imported, close the command window.

### ***Group File Import Text File Format***

To use this tool, create a file using a plain text editor, such as Notepad. The file contains group names followed by a list of email addresses of the users in each group. You can also use the asterisk (\*) wildcard to allow address matching. The following text illustrates the file format to use:

<b>Element</b>	<b>Description</b>
[New Group]	Group name
Jim@example.com	Email address
John@example.com	Email address
q*@example.com	Several email addresses specified using wildcard

### ***Group File Import Command Format***

Use the following syntax and options to issue the command:

```
GroupFileImport.exe [options] {-f inputfilename}
```

The following example imports user addresses from `mygroups.txt`, and merges the addresses into the group if the group name already exists.

```
GroupFileImport.exe -m -f mygroups.txt
```

<b>Option</b>	<b>Use</b>
-h {computer name or identifier}	Array Manager name or IP address. Defaults to local host.

Option	Use
-p {IP Port}	Array Manager port (defaults to 19001) .
-n {text}	Text string prefixed to all group names at import, such as <i>File Group</i> :
-m	Merge imported data. <b>Warnings:</b> <ul style="list-style-type: none"> <li>• <i>If a group in the import file has the same name as an existing group, existing items in the group are not deleted. MailMarshal SMTP adds new items from the import file group.</i></li> <li>• <i>Using the command without the -m switch deletes all members from an existing group before importing the file contents.</i></li> </ul>
-v	Verbose mode. Generates warnings about individual group members for troubleshooting.
-u {user name}	User name used to connect to the Array Manager server. Defaults to the logged-on user.
-d {domain}	Domain in which the user name is found.
-k {password}	Password associated with the user name.
-?	Prints help for the command help.

## USING THE CONFIGURATION EXPORT TOOL

The MailMarshal SMTP Configuration Export Tool is a command line tool that allows you to export and import MailMarshal SMTP configuration settings from a command line interface or batch file. The input and output of this command is a \*.xml file that contains the MailMarshal SMTP configuration information.

To use the tool, log onto the Array Manager computer with a Windows account with permissions to modify the Windows Registry (for example, as a member of the Windows administrator group on the system). Open a command prompt to run the command.

## ***Export Configuration Command Format***

The syntax and options of the `MMEExportCfg.exe` command are as follows:

```
MMEExportCfg.exe [options] {filename}
```

The following example exports the MailMarshal SMTP configuration to `myconfig.txt` and merges specified settings if the setting name already exists.

```
MMEExportCfg.exe -m -f myconfig.txt
```

<b>Option</b>	<b>Use</b>
-i	Imports the configuration from the specified file. Without the -i option, the command <b>exports</b> the configuration.
-f	On export, filters out local settings specific to the specific MailMarshal SMTP instance; global settings are exported. One use of this setting is to copy email policy from one MailMarshal SMTP installation to another.
-m	Merge the imported policy. If a setting is not present in the import file, the existing setting remains in place. Using the command without the <b>-m</b> option clears all settings that are not in the import file.
-c	Commit configuration after import.
-s:{ <i>computer name or identifier</i> }	Array Manager name or IP address. Defaults to Local host
-p:{ <i>IP Port</i> }	Array Manager port. Defaults to 19001.



---

## Chapter 10

# Delegating Spam and Quarantine Management

In some cases when MailMarshal SMTP quarantines an email message as suspicious, the recipient or sender wants the message to be released to its destination. If an organization generates a large number of these cases, the email administrator may not have the time required to review them. This situation is likely to arise with messages that MailMarshal SMTP has classified as spam.

MailMarshal SMTP provides several options that allow the administrator to delegate the responsibility for reviewing these messages and taking action:

- Departmental administrators or help desk personnel can have permission to process the messages in selected quarantine folders, using the MailMarshal SMTP Console or Web Console.
- Each email user can receive a daily summary of their incoming messages that have been quarantined, through MailMarshal SMTP digest emails.
- Each email user can have permission to review and release messages quarantined in one or more folders, through the MailMarshal SMTP Spam Quarantine Management Website. This facility is specifically designed to allow users to review messages that have been classified as spam, but it can be used for other classifications. It also allows each user to refine the spam classification by maintaining personal lists of safe and blocked senders.
- Where a policy requires a small number of messages to be held for review, users can receive notice of each message and release it by email using the MailMarshal SMTP Message Release external command. For more information, see “Using the Message Release External Command” on page 312.

## SETTING UP CONSOLE ACCESS

MailMarshal SMTP controls access to the features of the Console through Access Control Lists (ACLs) that contain Windows user information.



**Note:** You can grant users or groups, such as a help desk user group, the permissions *Read* and *Release*. These permissions allow group members to manage messages without seeing the content of messages.

For general information about setting Console security and access, see “Setting Console Security” on page 246.

### **To allow a user to use the MailMarshal SMTP Console to release messages from quarantine:**

1. Grant the user the Console permission *Console and Folder Connect*.
2. For each quarantine folder the user is allowed to manage, grant the appropriate permissions.

## SETTING UP SPAM QUARANTINE MANAGEMENT FEATURES

The MailMarshal SMTP Spam Quarantine Management system includes a website that allows users to review and release email quarantined in one or more folders that you specify. The website also allows each user to maintain lists of allowed senders and blocked senders. You can use these lists in MailMarshal SMTP rules to help determine whether email sent to that user is spam.

For information about setting up the Spam Quarantine Management Website, see “Installing and Customizing Web Components” on page 70.

## Spam Quarantine Management Windows

The Spam Quarantine Management Website includes the following pages:

### Log In

Allows a user to enter an email address and password to log in to the Spam Quarantine Management Website. Also allows a user to request a login and to request a new password. MailMarshal SMTP only uses this page if you configure the site to use authentication by email address and password.

### Home

Allows a user to view a list of email blocked since their last visit, and summary charts of blocked and good email (if allowed by the administrative settings).

### Blocked Mail

Allows a user to review a list of email quarantined in one or more folders. The user can view, release or delete each message. The user can also add the sender address to the blocked or safe senders list (if allowed by the administrative settings). If more than one folder is available through this site, the page shows a list of folders the user can review.

### Message Details

Allows a user to view the body and additional details of a message from the list of blocked email. The user can release the message or delete the message, and add the sender to blocked or safe senders.

### Manage Senders

Allows a user to add, edit, or delete entries in lists of safe and blocked email addresses. MailMarshal SMTP uses these lists in the rule condition “Where sender is/is not in recipient’s safe senders list” and “Where sender is/is not in recipient’s blocked senders list.”

## User Settings

Allows a user to configure site and address options.



**Note:** *Some options can be globally enabled or disabled by the administrator (using options on the Administrator tab of the site).*

- Set the site look and feel.
- Add or delete entries in a list of email addresses that they can manage using this login (if allowed by the administrative settings). Before adding a requested address to the list, MailMarshal SMTP requests confirmation by sending a message to the email address. The user must click a link in the message and confirm the request.
- Delegate the power to review their blocked email to one or more other users. The delegates will also be able to edit the user's blocked and safe senders lists. The delegates can choose which user's email to review using a list at the top of the page. Depending on the site authentication setting, delegation is by email addresses or Windows user names.
- Choose to receive, or not receive, specific digests (if permitted by the global settings of each digest).

## Change Password

Allows a user to change the password associated with their login (email address) for this site. MailMarshal SMTP only uses this page if you configure the site to use authentication by email address and password.

## Administrator

Allows Site Administrators to perform configuration and administration functions for the Spam Quarantine Management site:

- configure site settings
- globally enable and disable use of site features including the charts, safe senders and blocked senders, email address management, folder counts, and "all folders" view.
- delete users



- view and act on blocked mail for any user
- edit the safe, blocked, delegate, and owned email addresses for any user

### Help

Each page includes a link to a Help window that provides additional information about fields and functions.

## Setting Up Folders and Templates

The primary use of the Spam Quarantine Management Website is to allow users to review messages that MailMarshal SMTP has quarantined as spam. You can configure the site to manage one or more folders used for this purpose. You can also configure the site to manage folders that are used for other purposes.

Each folder managed by the Spam Quarantine Management Website can contain either messages sent to local users or messages sent by local users, but not both.

### To set up folders to manage spam with the Spam Quarantine Management Website:

1. Create or edit a MailMarshal SMTP folder. See “Using Email Folders and Message Classifications” on page 212.
2. On the Options tab of the folder properties, choose the setting **Enable End-user Management for this folder**.
3. Choose the setting **Folder is used to manage inbound messages**.
4. *If you want each user to receive a digested notification* of messages addressed to them that have been quarantined in this folder, create a message digest that includes the folder. See “Setting Up Message Digests”.
5. Repeat Steps 1 to 4 for each folder you want to set up for Spam Quarantine Management.

## Setting Up Message Digests

MailMarshal allows you to send email summaries to users, notifying them about messages addressed to them that MailMarshal has quarantined. Users can review and release the messages directly from the digest email. Digests are often used for the same folders that are available for end user management in the SQM website, but you can also create digests to allow message releasing for other folders.

A digest only lists messages that have not been included in a previous digest.

A message digest can

- Include information about messages in one or more folders
- Include or exclude messages from digesting, by checking user groups
- Be generated using one or more schedules. Each schedule causes the digest to be generated at a specified time on one or more days each week
- Use a specified email template. To learn more about templates, see “Creating Digest Templates” on page 198.
- Send digest emails to each user with undigested email in the folder, or send all digest emails to a specified address.
- Allow users to subscribe or unsubscribe from the digest using the SQM website or release webpage.

To work with message digests in the Configurator, select Message Digests from the left pane menu tree.

### *Creating Message Digests*

You can create as many digests as your policy requires.



**Note:** *The New Message Digest Wizard creates a digest using the most common options. Additional advanced options, such as multiple schedules, user group settings, and subscription settings, are not presented in the Wizard. To set advanced options for a Digest, edit the Digest after completing the Wizard.*

**To create a message digest:**

1. On the Action menu, click **New Message Digest**. to start the New Message Digest Wizard.
2. On each screen in the Wizard, specify the appropriate values. For more information about fields on a window, click **Help**.
3. Click **Finish**.

***Editing Message Digests***

You can edit the name and features of a digest, including the folders digested. You can set advanced features of the digest by editing it. Advanced features include multiple schedules, selection of email to digest by user group, and the recipient of digest emails.

**To edit a message digest:**

1. Double-click the digest name in the right pane of the Configurator to view its properties on a tabbed window.
2. On each tab, specify the appropriate values. For more information about fields on a tab, click **Help**.
3. Click **OK**.

***Deleting Message Digests***

You can delete a digest if you do not want to produce the digest emails.

**To delete a message digest:**

1. Select the digest name in the right pane of the Configurator.
2. Click the **Delete** icon in the toolbar.

## Setting Up Rules

MailMarshal SMTP places email in quarantine folders through rule action.

### To set up spam Quarantine rules:

1. Create MailMarshal SMTP rules to move spam messages into each folder you have created. If you are using the default configuration provided with MailMarshal SMTP, rules are included in the Spam policy group to move spam messages into several folders.
2. Within the rule or rules, use the condition “Where the sender is in the recipient’s allow list.” Configure the rule so that messages that meet this condition are not quarantined as spam.
3. Within the rule or rules, use the condition “Where the sender is in the recipient’s block list.” Configure the rule so that messages that meet this condition are quarantined as spam.



**Notes:** *If you are using the default configuration provided with MailMarshal SMTP, the rules included in the Spam policy group use these conditions.*

- *The user safe and block list conditions use the Safe Senders and Blocked Senders lists maintained within the Spam Quarantine Management website. If the SQM website is not in use, or if you choose to disable these lists (using the Administrator access to the SQM website), then these rule conditions will have no effect.*
4. When a user releases a message from the SQM website, MailMarshal SMTP continue processing the message as specified in the rule that moved the message to the folder. For more information, see “Move the message” on page 166.

## Setting Up Spam Quarantine Management for Other Folders

You can configure any MailMarshal SMTP folder to be managed through the Spam Quarantine Management Website.



**Note:** *Each folder can be used for inbound or outbound messages, but not both.*

### To set up folders to manage other messages with the Spam Quarantine Management Website:

1. Create or edit a MailMarshal SMTP folder. See “Using Email Folders and Message Classifications” on page 212.
2. Choose the setting **Enable End-user Management for this folder**.
3. Choose the setting **Folder is used to manage inbound messages** or **Folder is used to manage outbound messages** as appropriate.



**Tip:** *When you create rules to quarantine messages in these folders, **be sure to direct inbound and outbound messages to the correct folders**. This setting is used to determine the recipient of the email for digesting and the Spam Quarantine Management website.*

4. **If you want each user to receive a digested notification** of messages addressed to them that have been quarantined in this folder, create a message digest that includes the folder. See “Setting Up Message Digests” on page 308.
5. Repeat Steps 1 to 4 for each folder you want to set up for Spam Quarantine Management.

# USING THE MESSAGE RELEASE EXTERNAL COMMAND

Some MailMarshal SMTP administrators set up rules that quarantine small volumes of email for specific reasons. For instance, an Acceptable Use Policy could require that the sender or an administrator must “click to confirm” before sending or receiving some types of content.

MailMarshal SMTP provides a message release function for these situations. Message Releasing allows MailMarshal SMTP to send an email notification when it quarantines a message. Simply by replying to the notification, a user can release the original message from quarantine.

## To use automatic message release:

1. Create or modify a MailMarshal rule which moves certain messages to a folder.
2. In this rule, include a rule action which sends a notification message. The body of this message must contain the variable `{ReleaseProcessRemaining}` or `{ReleasePassThrough}`.
  - The `{ReleaseProcessRemaining}` variable causes the message to be processed through additional rules, as specified in the Release Action of the rule that quarantined it. For more information, see “Move the message” on page 166. This option is more secure and recommended.
  - The `{ReleasePassThrough}` variable causes the message to be queued for delivery with no further processing of rules.

See the pre-configured template Automatic Message Release Outbound for an example.



**Notes:** *The message template must include a plain text message body. It may include a HTML body as well.*

- *The From address must be one which guarantees that replies will pass through MailMarshal SMTP. The address need not be valid but it must be well-formed.*

To process message release requests, create a MailMarshal SMTP rule similar to the following:

```
Where addressed to MessageRelease@Release.example.com
Run the external command Message Release
And write log message(s) with Release Requests
And delete the message
```

The message classification “Release Requests” is pre-configured.

Automatic Message Release should be used sparingly as it tends to defeat the purpose of MailMarshal SMTP.

If MailMarshal SMTP is used in an array with separate Array Manager and processing servers, the Message Release external command must run using a Windows credential that the Array Manager can validate. You can enter specific account credentials for the Message Release external command, using command line parameters in the External Command definition. See “Message Release Options.”

If you want to be notified of failed message release attempts, you can run the external command as a rule condition rather than an action. The Message Release executable returns 0 on success and 1 on failure.

## ***Message Release Options***

The Message Release external command has the following syntax:

```
MMReleaseMessage [-u username] [-p password] [-d domain]
[-r recipient] [-I] {MessageName}
```



**Note:** {MessageName} is a MailMarshal variable. The braces are part of the variable syntax. You must include this literal string in the command parameters.

To use the options, edit the external command definition. In the properties, change the parameters field to include the required options.

### The options are further described as follows:

```
-u {username}
-p {password}
-d {domain}
```

Use these options to run the external command as a specific Windows user. This functionality may be required for instance on Windows Server 2003 SP2 with enhanced security configuration.



**Note:** You must include the password value.

```
-I leave message in folder
-r send only to named recipient
```



By default the Message Release executable releases the message to all recipients and deletes the message after releasing it. Using these options can result in a message being sent to a user more than once. You can use two parameters to modify release behavior:

- To leave a copy of the message on the server after releasing it, change the parameters field to include `-l {MessageName}` (the parameter is a lower case letter L).
- You can also configure the message release facility to release the message only to the user requesting it. Typically you would use this option in the case of incoming messages addressed to more than one user. To implement this function, change the parameters field to include `-r {From}`. The message will be released only to the email address from which the request was sent. This need not be one of the original recipients. The message will be left on the server and can be released again.



---

## Chapter 11

# Reporting on MailMarshal SMTP Activity

The MailMarshal SMTP Reports application allows you to generate reports based on the information MailMarshal SMTP logs as it processes email messages. You can choose from a wide range of reports covering email throughput, specific content, and threat information. You can produce both overall summaries and per-user information.



**Note:** *The structure of the MailMarshal SMTP reporting database, and the reporting queries, have changed significantly in MailMarshal SMTP version 6.X. If you have imported data from a version 5.X MailMarshal SMTP database, reports may show different results to the equivalent reports in the earlier version.*

M86 Security also provides an alternative reporting interface, the Marshal Reporting Console. The Marshal Reporting Console is based on SQL Server Reporting Services, and offers scheduled generation and automatic delivery of reports. For more information about this application, see the M86 Security website or contact M86 Security.



**Note:** *The data retention and grouping information in this chapter also applies to reports generated through Marshal Reporting Console.*

# DATA RETENTION AND GROUPING

The data available for reports, and grouping of certain data items, is configured through the MailMarshal SMTP Configurator.

## To configure reporting options:

1. Open the MailMarshal SMTP Configurator.
2. On the Tools menu, click **MailMarshal Properties**.
3. Click **Reporting**.
4. When you have completed changes to Reporting options as described in the next sections of this chapter, click **OK** and then commit the MailMarshal SMTP configuration to effect the changes.

## Configuring Data Retention

You can adjust the length of time MailMarshal SMTP retains logging records. Best practice is to retain enough data to allow reporting on several months of email traffic. You can also reduce the size of your MailMarshal SMTP database by reducing the retention time.

If you archive messages for longer than the logging retention time, MailMarshal SMTP will retain basic database records about each archived message for as long as the archives are retained. This information is necessary to allow viewing of the messages in the Console. For more information about backing up and restoring messages in quarantine folders, see the M86 Security Knowledge Base.

**To configure your reporting data retention period:**

1. The General Options area of the Reporting section shows the length of time for which MailMarshal SMTP will retain logging data.
2. To change the retention time, enter a number of days.
3. Click **OK**.

## Configuring Reporting Groups

Information about spam, viruses, and Blended Threat URLs is likely to be logged in varying classifications and folders. To allow unified reporting on these categories, MailMarshal SMTP allows you to specify the folders and classifications you are using for each of these types of content. These groups affect the display on the Dashboard page of the Console, the Spam Overview report, the Virus Overview report, and the two virus detail reports.

**To configure the reporting groups:**

1. The Reporting Group area of the Reporting section shows the folders and classifications that are included in each reporting group.
2. To change the items included in a group, click **Modify** to open the Edit Reporting Group window.
3. Select the items you want to include, then click **OK** to return to the Reporting section of MailMarshal Properties.



**Note:** *Ensure that the folders and classifications you select are relevant to the purpose of the group. Otherwise, results based on the group will be meaningless.*

4. To show counts for the top five quarantine folders on the Dashboard page of the Console, check the box **Display Message Count**.

## CONNECTING TO THE DATABASE

MailMarshal SMTP Reports uses a direct connection to the MailMarshal SMTP database, which is hosted on a Microsoft SQL Server or SQL Express. To generate reports, you must be able to connect to the database. If the database is separated from the client workstation by a firewall, connect using TCP and open the Microsoft SQL Server port through the firewall. By default this is port 1433.

### To connect to the database:

1. Run the MailMarshal SMTP Reports application in the MailMarshal program group.
2. ***If this is the first time MailMarshal SMTP Reports has been run on this workstation, or the database connection information has not been saved***, MailMarshal SMTP Reports displays a window requesting connection information. Enter the appropriate information to connect to the database. In the SQL Server Name field you can use the syntax `servername[\instance][, port]`.



**Note:** *If you use Microsoft SQL Server named instances, use the instance parameter rather than the port parameter.*

3. If you want to connect to a different database, in the left pane of MailMarshal SMTP Reports select the item **MailMarshal Reporting**. From the Action menu, select **Database**. Enter the appropriate information to connect to any database.

## GENERATING REPORTS

Within MailMarshal SMTP Reports, reports are organized in folders. The default folders group reports according to functions, such as classification reports, bandwidth reports, and virus related reports.

## Available Reports

To view the list of available reports, expand the items in the left pane. The **Description** column of the right pane gives basic information about each folder and report.

To view the full definition of a particular report, select it, and then choose **Properties** from the Action menu.

The properties are shown in a Report Properties window with four tabs.

- **General:** gives the report name, as shown in the MMC, and a more complete description.
- **Parameters:** gives the report title, as it will be seen when the report is generated, and shows the default parameters that will be used.
- **Report:** Shows information about the report definition file and the DLL it is stored in.
- **Select:** You can select a new report definition file from the list. Choosing a new file will effectively reset all features and is generally not recommended.

If the check box **Request parameters before running report** is selected, the parameters detail will be presented to the user each time the report is generated. If this box is not selected, MailMarshal SMTP will not request parameters when the report is generated.

To view and change the parameters using the parameters detail window, click **Edit**.

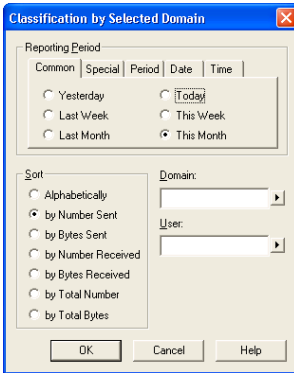
***Tip:** You can save a specific instance of a report, such as “all traffic last month from example.com”, by editing the parameters and clearing the **Request Parameters** box. You can run this report quickly by double-clicking on the report name in the main Reports window.*

## Entering Report Parameters

Enter your report parameters to specify the data that makes up the report.

## To generate a report:

1. Open the Reports application.
2. In the left pane expand the required reports folder.
3. In the right pane, select a report, and then click **Open** on the Action menu. By default MailMarshal SMTP displays a parameter detail window similar to the following:



4. Specify the appropriate values. For more information about fields on a window, click **Help**.



**Note:** If MailMarshal SMTP Reports does not display the parameter detail window, the report is configured to run without requesting parameters. You can change this behavior by selecting the report then clicking **Requests Parameters** on the Action menu.

5. Click **OK** to view the report.

The title of the parameter detail window shows the title of the report as it will be generated. To change the title use the Parameters tab of the Report Properties window. For more information about the available parameters, see “Available Parameters.”



## Available Parameters

Each MailMarshal SMTP report has a different set of parameters. For more information about the parameters of a specific report, see Help for the specific parameter window.

## NAVIGATING THE REPORT WINDOW

A typical MailMarshal SMTP report window is shown below:

**Classification by Selected Domain**

All Domains  
All Users  
Sorted by Number Sent  
For month commencing 01-Apr-2010  
Printed: 06-May-2010 at 10:12

Classification	Domain	Sent		Received		Total	
		Msgs	MB	Msgs	MB	Msgs	MB
<b>Spam - Explicit</b>		895,827	2,826.99	1,041,969	3,340.17M	1,927,096	6,167.16
	exa05.example.com	338,546	1,073.88	0	0.00	338,546	1,073.88
	exa07.example.com	302,193	964.37	0	0.00	302,193	964.37
	exa06.example.com	246,898	786.74	0	0.00	246,898	786.74
	ext2.example.com	0	0.00	347,287	1,111.57	347,287	1,111.57
	ext3.example.com	0	0.00	346,104	1,110.84	346,104	1,110.84
	ext4.example.com	0	0.00	348,678	1,117.76	348,678	1,117.76
<b>Delivered successfully</b>		199,925	7,730.07	228,341	8,879.81	422,266	16,609.88
	exa02.example.com	71,128	3,089.45	269	1,460.23	71,397	4,549.68

The report window provides several options to customize the view and see additional details. The Help menu for the report window includes two choices: general help and help about the specific report.

## Toolbar Options

- **Close Current View:** close the drill-down tab currently showing.
- **Print:** print a copy of the report, or selected pages. (Printer setup is available from the File menu)
- **Toggle group tree:** show a list of available detail items in a separate pane. Double-click any of these items to jump to it in the main report. If the item is a group, click the + icon to view the members of the group.
- **Magnification:** choose the magnification of the report on screen.
- **Page selector:** shows the number of pages in the report. Choose the page to view.



**Note:** *The scroll bar in the report window is limited to the current page. Use the page selector to move between pages.*

- **Stop button** (available while report is being generated): Stop generating the report. Optionally show the partial report.

## EXPORTING REPORTS

MailMarshal SMTP Reports can be exported (saved) in a variety of formats provided by the Crystal Reports engine. The presentation quality varies depending on the format you select. In general the best formats to use are: Crystal Report, DHTML, text, Excel, and RTF.

Begin exporting a report by right-clicking on the report name and choosing **Export**, or by clicking the Export icon from the report window toolbar.



**Note:** *Drill-down pages are only available in the Crystal Report 8.0 export format. All other export formats show only the main report view.*

## ***Export Options***

Selecting **Export**, either from the report window or by right-clicking on a report name, opens the export options window. You can also open this window by selecting a report name and choosing **Export Options** from the Action menu. The options you select become the defaults for the report instance.

On the first page of the Export Options window, choose how to create the export:

- **File** saves the export as a file. The reports engine enters a name by default. To select a specific name, use the browse button or type a file name in the field.
- **Application** opens the export directly in the required application (such as Internet Explorer or Lotus 123). Clear the check box **Use Temporary File** to save the data in a permanent named file as well.
- **Email** attaches the exported data to an email message using the default email application.

Depending on the type of export chosen, you may have additional options to choose from.

## ***Email Options***

The report will be attached to the email as a file of the type you choose on the export options window.

- **Send to:** Enter the email address to which the message should be sent.
- **Copy to:** Optionally enter an email address to which the message should be CC'd.
- **Subject:** Optionally enter a subject for the email message.
- **Message:** Optionally enter a message body describing the attachment.

## ***HTML Options***

Use these options when exporting a report in HTML format.

- **Generate navigation buttons:** The engine will add links at the bottom of each page to jump to the first, next, previous, or last page of the report.
- **Create all output on one page:** The engine will create a single HTML document for all output. Page divisions will show as lines.

## ***Pagination Options***

When exporting a report to paginated text set **Lines per page** to the number of output lines between page break characters.

## ***Separator Options***

Use these options when creating a values text file (character separated values, comma separated values, data interchange format, and tab separated values).

- **Format numbers as in report:** The engine will output numbers with text formatting (such as comma separation of thousands). Clearing this box causes numbers to be output in a basic format.
- **Format dates as in report:** The engine will output dates with text formatting. Clearing this box causes dates to be output in a basic format.

You can select from the following additional options for character separated values only:

- **Field separator:** Determines the character (or characters) marking the boundary between two fields. A commonly used value is the comma. In addition to printable characters, special separators you can choose include:

Field Entry	Separator used
\t	Tab character
\n	New Line character
\r	Carriage Return
\0	NUL character (Hexadecimal 00)
\\	\ (backslash)
\xHH	Any character (two hexadecimal digits)

- **String delimiter:** Determines the character (or characters) marking the beginning and end of field text. You can use the same values as for field separators. A commonly used value is the quote character. This field can also be blank, in which case the engine will not add a field delimiter.



---

## Appendix A

# Wildcards and Regular Expressions

MailMarshal SMTP supports a simple wildcard syntax when you enter several types of information including local domains, user groups, and report parameters.

MailMarshal SMTP also uses a full Regular Expression syntax for matching and substitution in Header Rewrite rules.

## WILDCARD CHARACTERS

MailMarshal SMTP allows wildcard entries in the following contexts:

- Local domains. See “Running the Configuration Wizard” on page 56.
- User and Group matching for policy groups and rules. See “Understanding User Matching” on page 131.
- Receiver HELO name matching. See “Where sender's HELO name is/is not criteria” on page 158.
- The Console search and filtering options. See “Using the MailMarshal SMTP Console” on page 231.
- BTM exclusions. See “MailMarshal Properties - Advanced” on page 292.
- Report parameters. See “Entering Report Parameters” on page 321.

In each of these types of entry, MailMarshal SMTP supports this syntax:

Character	Function
*	Matches any number of characters
?	Matches any single character
[abc]	Matches a single character from a b c
[!abc] or [^abc]	Matches a single character except a b or c
[a!b^c]	Matches a single character from a b c ! ^
[a-d]	Matches a single character in the range from a to d inclusive
[^a-z]	Matches a single character not in the range a to z inclusive

The table below gives some examples of results of the wildcard syntax.

Pattern	matches
*.ourcompany.com	pop.ourcompany.com hq.ourcompany.com <i>etc.</i>
*.mail[0-9].ourcompany.com	mail5.ourcompany.com <i>but not</i> maila.ourcompany.com
mail[!0-9].ourcompany.com	mails.ourcompany.com <i>but not</i> mail3.ourcompany.com



**Note:** The !, -, and ^ are special characters only if they are inside [ ] brackets. To be a negation operator, ! or ^ must be the first character within [ ].



# REGULAR EXPRESSIONS

MailMarshal SMTP uses regular expressions in header matching and rewriting rules. For more information about these rules, see “Standard Rules” on page 129. MailMarshal SMTP also uses regular expressions in category scripts. For more information about category scripts, see the white papers “MailMarshal SMTP Anti-Spam Configuration” and “MailMarshal SMTP Advanced Anti-Spam Configuration,” available from the MailMarshal SMTP support page at [www.m86security.com](http://www.m86security.com).

MailMarshal SMTP implements a full-featured regular expression syntax. Full documentation of this syntax is beyond the scope of this manual. For additional documentation and links to further information, see M86 Security Knowledge Base article Q10520.

This appendix provides limited information about some commonly used features and some extensions specific to MailMarshal SMTP.

## Shortcuts

The arrow to the right of each field on the matching/substitution page of the header rule wizard provides access to some commonly used Regular Expression features.

Selection	Inserts	Usage
Any Character	.	Matches any single character.
Character in range	[ ]	Enter a range or set of characters to be matched within the brackets. For instance, to match lower case characters you could enter a-z between the brackets.
Character not in range	[^]	Enter a range or set of characters after the ^. Matches any character not in the set.
Beginning of line	^	Text to the right of the ^ will only match if found at the beginning of the line.

Selection	Inserts	Usage
End of line	\$	Text to the left of the \$ will only match if found at the end of the line.
Tagged expression	( )	The content within the parentheses will be considered as a single expression for repeat purposes. This expression will be saved for use within the substitution field.
Or		The field will be matched if it matches either the expression before the   or the expression after the  .
0 or more matches	*	The expression before the * will be matched if it is repeated any number of times, including zero.
1 or more matches	+	The expression before the + will be matched if it is repeated at least once.
Repeat	{ }	Enter a number or two numbers separated by a comma within the braces. The expression before the braces will be matched if it is repeated the number of times specified. See "Repeat Operators * + ? {}" on page 333.
Whitespace	[:space:]	Matches a single whitespace character (space, tab, and so on.).
Alphanumeric character	[:alnum:]	Matches a single letter or number character.
Alphabetic character	[:alpha:]	Matches a single letter character.
Decimal digit	[:digit:]	Matches a single number character 0-9.

## Reserved Characters

Some characters have special meanings within regular expressions.

### *Operators*

The following characters are reserved as regular expression operators:

\* . ? + ( ) { } [ ] \$ \ | ^

To match any of these characters literally, precede it with \

For example, to match marshal . com enter Marshal \. com

## ***Wildcard Character .***

The dot character (.) matches any single character.

## ***Repeat Operators \* + ? {}***

A repeat is an expression that occurs an arbitrary number of times.

An expression followed by \* can be present any number of times, including zero. An expression followed by + can be present any number of times, but must occur at least once. An expression followed by ? may occur zero times or once only. You can specify a precise range of repeated occurrences as a comma-separated pair of numbers within {}. For instance,

ba\* will match b, ba, baaa, etc.

ba+ will match ba or baaaa for example but not b.

ba? will match b or ba.

ba{2,4} will match baa, baaa and baaaa.

## ***Parentheses ( )***

Parentheses serve two purposes:

- To group items together into a sub-expression. You can apply repeat operators to sub-expressions in order to search for repeated text.
- To mark a sub-expression that generated a match, so it can be used later for substitution.

For example, the expression (ab)\* would match all of the string

ababab

The expression “ab” would be available in a variable (tagged expression) with a name in the range \$1...\$9 (see the matching and substitution examples in following sections).

## ***Alternatives***

Alternatives occur when the expression can match either one sub-expression or another. In this case, each alternative is separated by a |. Each alternative is the largest possible previous sub-expression (this is the opposite to repetition operator behavior).

a(b|c) could match ab or ac

abc|def could match abc or def

## **Examples**

The following sections show examples of matching and substitution strings.

### ***Matching***

The expression

```
(.+)@(.)+\.ourcompany\.com$
```

will match a sequence of 1 or more characters followed by an @ followed by another sequence of 1 or more characters, followed by .ourcompany.com at the end of the field.

That is, it will match john@host.ourcompany.com and john.smith@host.subdomain.ourcompany.com but not peter@host.ourcompany.com.au

### ***Substitution***

Using the example given in the preceding section, the substitution expression

```
$1@$2.co.uk.eu
```

would yield `john@host.co.uk.eu`, `john.smith@host.subdomain.co.uk.eu` and `peter@host.ourcompany.com.au` respectively. The last result may be somewhat surprising, but data that does not match part of the regular expression is simply copied across.

## Map Files

MailMarshal SMTP allows substitution using regular expressions to search for an entry in text file known as a map file. Each line in the map file contains two values separated by a comma. If the search expression matches the first value in a line, MailMarshal SMTP substitutes the second value. If the search expression does not match the first value in any line, MailMarshal SMTP substitutes the search expression.

A typical use of map files is to redirect incoming email to arbitrary addresses. The following simple example modifies email addresses using a map file.

### *Map file*

```
john@domain.co.uk, john@domain2.co.uk  
peter@domain.co.uk, peter@host1.domain.co.uk
```

### *Search expression*

```
(. +)@domain\.co\.uk$
```

### *Lookup key*

```
$1@domain.co.uk
```

## ***Sample results***

The following table shows the matching addresses when the sample mapping file above is used.

<b>Input Email Address</b>	<b>Result</b>
john@domain.co.uk	john@domain2.co.uk
peter@domain.co.uk	peter@host1.domain.co.uk
alice@domain.co.uk	alice@domain.co.uk

---

## Appendix B

# Third Party Extensions

MailMarshal SMTP supports integration with a number of third party products that extend MailMarshal scanning and filtering capabilities. These products include virus scanning software, anti-spyware scanners, and image analysis software.

## IMAGE ANALYZER

Image Analyzer is a third party deep image analysis product that has been fully integrated into the MailMarshal content scanning engine. Integration with Image Analyzer allows MailMarshal to assess the content of images that pass through the email gateway. For usage details, see “Where the attached image is/is not/may be inappropriate” on page 151. M86 Security also provides integrated licensing for this product.

Because MailMarshal unpacks the content of a message, extracting the attachments and the content inside archive files, Microsoft Word documents, and other packed formats, Image Analyzer can scan the image content from all components of the target message.

The main target content that Image Analyzer attempts to detect is pornographic images. Image Analyzer uses a variety of techniques in its analysis to make this determination. It is important to note that detection of this type of content is not an exact science, and the level of technology available today means that there will be a degree of false-positive and false-negative detections. A number of control settings can be selected when creating a rule for image analysis, to help tune the results of the analysis.

## Why Would I Use Image Analyzer?

The primary goal for organizations deploying image analysis technology is to reduce legal liability and to ensure that company reputation is not compromised. Image Analyzer allows your organization to utilize leading technology, and provides evidence of due diligence in protecting your employees from receiving material that may be offensive or in some cases illegal. Executives in some countries can be held legally liable for not exercising due diligence in preventing material of this nature from entering or being stored on their systems.

Many organizations today are blocking all image content entering their organization to ensure that offensive material cannot enter. However, blocking all images can prevent the transmission of images that are required for business purposes.

Image Analyzer allows the organization to permit email transfer of legitimate images, and also to meet its legal obligations of due diligence and its more general moral obligations of protecting its employees from offensive material being delivered to them over a medium that they have no control over.



## What Results Can I Expect From Image Analyzer?

Image Analyzer has tested their technology with a wide range of image content that typically travels the Internet. The published results of this testing show a false-positive rate (the rate at which non-pornographic images are detected as inappropriate) of between 2% and 5%. The results also show a false-negative rate (the rate at which inappropriate images are not reported) of between 17% and 24%. Based on the type of content entering your organization you may see similar or slightly better results. These results compare favorably with other products on the market.

## How Does Image Analyzer Address the Issues?

Although today's technology does not allow Image Analyzer to provide 100% protection against inappropriate image content, use of Image Analyzer can help in two ways.

- Use of Image Analyzer can help to reduce liability by showing due diligence in providing an appropriate environment.
- The policy based functionality of MailMarshal allows social education on this issue within an organization. Individuals who exchange inappropriate material tend to do so repeatedly. MailMarshal can send a notification to the sender when it detects inappropriate content. Even if MailMarshal does not detect every instance of the material, the individuals will be educated that the content of email is being analyzed and monitored. The risk of action being taken, or social embarrassment, rapidly increases. Most users will cease to send material that they know is not acceptable under your organization's policy.

## VIRUS SCANNING SOFTWARE

MailMarshal SMTP provides high-throughput DLL interfaces to a number of well-known virus scanning products. In addition to a DLL interface, MailMarshal also provides integrated licensing and a customized upgrade component for the McAfee scanner (known as McAfee for Marshal). For usage details, see “Configuring Antivirus Scanning” on page 65 and “Stopping Viruses” on page 105.

Anti-virus software is considered a basic requirement for secure business networks. Integration of anti-virus scanning with MailMarshal allows checking for email viruses at the network boundary. This capability provides an added layer of protection beyond what desktop scanners can provide.

## ANTI-SPYWARE SCANNERS

MailMarshal SMTP provides high-throughput DLL interfaces, integrated licensing, and customized upgrade components for two anti-spyware scanners: PestPatrol and CounterSpy. These components are known as PestPatrol for Marshal and CounterSpy for Marshal.

Anti-spyware scanners provide significantly different benefits from virus scanners. Spyware behaviors can include key logging and other information theft, as well as annoying pop-ups and browser redirection. These behaviors are not usually classified as “viruses” because they do not usually attempt to spread themselves automatically and they do not destroy data or programs. However they can have a serious effect on security and productivity.

Integration of anti-spyware scanning with MailMarshal allows checking for email-borne spyware at the network boundary. This capability provides an added layer of protection beyond what desktop scanners can provide.

Configuration of anti-spyware scanners within MailMarshal uses the anti-virus configuration interface. For usage details, see “Configuring Antivirus Scanning” on page 65 and “Stopping Viruses” on page 105.

---

# Glossary

**access control list (ACL).** A table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file.

**Acceptable Use Policy (AUP).** Rules and regulations governing the use of organizational email and Internet browsing.

**Active Directory.** The directory service implemented in the Windows 2000 or later environment to store often accessed information. It contains information about users, groups, computers, organizational units, and domains.

**alert.** An indication of a significant event. Alerts are generated by MailMarshal services.

**appliance.** An integrated “plug and play” hardware/software solution. MailMarshal SMTP is available as an appliance installation.

**array.** A group of MailMarshal email processing servers that use the same policy.

**array manager.** A MailMarshal service that controls configuration for all email processing servers and connects to the MailMarshal database. Also, the server running the array manager service.

**attribute.** Computer characteristic, typically defined by a registry key or value.

**blended threat.** Security threat to a network using multiple vectors (for instance, a malicious URL sent by email).

**component.** Individual part of a MailMarshal implementation that performs a specific function. For example, an email processing server, Array Manager, or database is a MailMarshal component.

**computer name.** A name that uniquely identifies a computer on a network. The computer name cannot be the same as any other computer or domain name on the network. The network uses the computer name to identify the computer and to allow other users to access the shared resources on that computer.

**Configurator.** Interface that allows you to edit email policy and configure email delivery and server settings.

**Console.** Interface that allows you to monitor email traffic and manage quarantined email. Intended to be used by email administrators, managers, and help desk personnel.

**Denial of Service Attack (DoS).** An attempt to cause the target organization to lose access to common business services, such as email. In an email DoS attack, the attacker floods email servers with messages, causing the email servers to slow down or cease operation.

**Directory Harvest Attack (DHA).** An attempt to identify valid email addresses by sending randomly-addressed messages to an email server in a corporate network. When a message reaches a recipient without being bounced back, the attacker enters the valid address in a database used for sending spam.

**distinguished name.** An address format used to locate and access objects in an X.500 directory using the LDAP protocol. This format specifies the complete path to the object through the hierarchy of containers in a domain. Each distinguished name is unique. For example, a user object with the common name J. Doe in the organizational unit container called Users on the domain marshal.com might be represented as follows:

```
CN=JDoe, OU=Users, DC=Marshal , DC=com
```

**DNS.** See Domain Name Service (DNS).

**DLL.** A library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses these functions.

**DMZ.** A part of a local network that has controlled access both to the Internet and to the internal network of the organization. Servers that provide gateway services for an organization are typically located in a DMZ.

**DNS blacklist.** A service that provides an automated response through the DNS protocol. DNS blacklists typically attempt to list email servers that are associated with spamming, open relays, or other unacceptable behavior.

**Domain Name Service (DNS).** The Internet service that translates domain names into IP addresses.

**email processing server.** A MailMarshal server that accepts SMTP email messages and takes action as defined in the organizational email policy.

**Extended Simple Mail Transfer Protocol (ESMTP).** A standard that defines optional additions to the SMTP email protocol.

**event.** Any significant occurrence in the system or application that requires user notification or an entry to be added to an event log.

**event log.** A record of any event that happens on a server. In Windows, events are stored in the System, Security, or Application log.

**Extensible Markup Language (XML).** A data tagging language that permits the storage and interchange of structured data.

**fault tolerance.** The ability of a product to respond to a catastrophic event (fault) that ensures no data is lost and that any work in progress is not corrupted.

**firewall.** A security system that is placed between the Internet and the private network of an organization, or within a network, and only passes authorized network traffic.

**folder classification.** An entry indicating a quarantine folder name written to the MailMarshal database when a file is moved to a quarantine folder. MailMarshal creates the database entry automatically.

**hyperlink.** An emphasized portion of text on a window that, when clicked, opens another document or window.

**IIS.** See Microsoft Internet Information Services (IIS).

**Lightweight Directory Access Protocol (LDAP).** A network protocol designed to work on TCP/IP stacks to extract information from a hierarchical directory such as X.500. It is useful for searching through data to find a particular piece of information. An example of an LDAP directory is the Active Directory in Windows 2003 or later. Objects in an LDAP directory are identified by their distinguished names.

**local area network (LAN).** A group of computers in the same place that are connected and typically have the same network operating system installed. Users on a LAN can share storage devices, printers, applications, data, and other resources.

**mailbox.** A disk storage space assigned to a user account to receive incoming email messages.

**MDAC.** See Microsoft Data Access Components (MDAC).

**message classification.** Classification action defined in a rule as `Write Log message with x`.

**Microsoft Data Access Components (MDAC).** A set of network libraries and programming interfaces designed to allow client applications to connect to data providers such as SQL Server databases.

**Microsoft Internet Information Services (IIS).** A Web server application for Windows operating systems.

**Microsoft Management Console (MMC).** A common interface designed to host administrative tools for networks, computers, services, and other system components.

**Multi-Purpose Internet Email Extensions (MIME).** A standard that permits transmission of content other than text through SMTP email.

**Microsoft SQL Server Desktop Engine (MSDE).** A freely distributable limited version of SQL Server 2000. Note that MSDE is no longer supported by MailMarshal SMTP.

**open relay.** An email server that accepts messages from any server for delivery to any other server. Open relays are often exploited by spam senders.

**permissions.** Authorization for a user to perform an action, such as sending email messages for another user or posting items in a public folder.

**Post Office Protocol 3 (POP3).** The standard protocol used by email client software to retrieve email messages from a mailbox.

**queue.** A storage structure in which a set of items are held until they can be processed. For example, when MailMarshal receives email messages, the messages are stored in a queue until the MailMarshal Engine can process them.

**registry.** A database repository for information about the computer configuration. The database is organized in a hierarchical structure of sub trees and their keys, hives, and value entries.

**regular expressions.** Search criteria for text pattern matching that provide more flexibility than simple wildcard characters.

**relaying.** Sending an email message to an email server for delivery to another server. See *open relay*.

**remote procedure call (RPC).** A standard protocol for client server communication that allows a distributed application to call services available on various computers in a network.

**reputation service.** A service that provides an automated response that classifies the source of an email message. Reputation services are usually implemented as DNS blacklists.

**scalability.** Ability to distribute loads across multiple servers, allowing for greater accessibility and balanced traffic.

**Sender ID.** A standard for validation of the source of an email message, based on special DNS records. Typically used for anti-phishing checks.

**Sender Policy Framework (SPF).** A standard for validation of the source of an email message, based on special DNS records. Typically used for anti-phishing checks.

**service account.** In Windows NT it is a user account that a service uses to log on to Windows NT. The account must have the specific rights and permissions required by that service.

**Simple Mail Transfer Protocol (SMTP).** A member of the TCP/IP suite of protocols. The standard governing email delivery over the Internet.

**SMTP.** See Simple Mail Transfer Protocol (SMTP).

**Spam.** Unsolicited email messages, usually of a commercial nature.

**SpamBotCensor.** A proprietary spam detection technology incorporated in MailMarshal. SpamBotCensor leverages the message analysis tools of SpamCensor to efficiently identify spam that is generated by botnets.

**SpamCensor.** A proprietary spam detection technology incorporated in MailMarshal. SpamCensor includes a multi-faceted message analysis tool and regular definition updates.

**SpamProfiler.** TA proprietary spam detection technology incorporated in MailMarshal. SpamProfiler is a signature based system that operates during message reception and includes regular definition updates.

**Spam Quarantine Management Website.** Interface that allows a user to review and release their email messages that MailMarshal has quarantined.

**split message.** A message for multiple recipients that MailMarshal divides into copies. MailMarshal processes each copy differently, according to the rules indicated for a specific recipient.

**spoofing.** Disguising the sender address of an email message to make it appear as though it is from another person, usually for malicious reasons.

**SQL Express.** A freely distributable limited version of SQL Server.

**SQL Server.** The Microsoft enterprise database server software.

**Structured Query Language (SQL).** A programming language used to retrieve information from a database.

**TextCensor.** The lexical analysis engine included in MailMarshal. TextCensor allows you to scan email messages and attachments for complex text content, using Boolean and proximity operators and numerical weighting.

**Transport Layer Security (TLS).** A protocol intended to secure and authenticate communications (such as email) across public networks by using data encryption.

**Web Console.** Interface that allows you to perform Console functions from any computer that can run Microsoft Internet Explorer. See *Console*.

**wildcard character.** A character in a search pattern that represents a number of arbitrary characters within the text being searched.

**X.500.** A global, hierarchical directory service. For example, a domain controller hosting Active Directory on a network running Windows 2003 or later provides an X.500 directory service.

**XML.** See Extensible Markup Language (XML).



---

# Index

## A

- Accept message 169
- Acceptable Use Policy 97, 192
- Accounts 116, 150, 157, 278
- Actions. *See* Rule Actions
- Active Directory 62, 177, 179, 180
- Add message users 166
- Administrative notifications 58, 104, 196
- Administrator email addresses 58
- Advanced options 292
- Alert History 245
- Aliases, email 279
- Anti-relaying 97, 109, 110, 149
- Anti-Spyware 65, 105, 212, 340
- Anti-Virus 107
  - supported software versions 39
- Appliance 11, 17, 38, 44, 45, 52, 65, 95, 212, 265, 279, 287, 292
- appliance 38
- Archiving 235, 318
- Array Manager 25, 48, 295
- Array of servers 24, 48, 282
- Array options
  - Delivery 277
  - Managing nodes 282
- Attachment fingerprints 140, 216
- Attachment parent 143
- Attachment size 144
- Attachments
  - Checking name 142
  - Checking parent type 143
  - Checking size 144

- Checking text 186
- Checking type 140
- Counting 146
- Scanning for viruses 137
- Stripping 162
- Unpacking depth 292
- Valid fingerprints 140, 165
- attack prevention 116
- automatic adaptive whitelisting 112

## B

- Back up
  - Configuration 260
  - Folders 318
  - Messages 318
  - TextCensor scripts 192
- Bandwidth required 142
- BCC 161
- Best practices 108, 133, 192, 278
- Blended Threats 139, 233, 319
- Block receipt 169
- Blocked Hosts 115

## C

- Category scripts 146
- certificates
  - creating and managing 290
  - TLS 289
- Classifications 162, 212, 213
- Commit configuration 89, 233, 234, 283

- Scheduling 89, 293
- Conditions. *See* Rule Conditions
- Configuration
  - Back up and restore 260
  - Importing and exporting 300
  - MailMarshal properties 88
- Configurator, MailMarshal 86
- configuring
  - DHA attack prevention 121
  - DoS attack prevention 117
- Connectors 177
- Console, MailMarshal
  - Security 246
  - Understanding 90
  - Web Console 92
- Continue Processing Rules 170
- Copy the message 160
- CounterSpy for Marshal 65, 105, 212, 340
- creating
  - TLS certificates 290
- Crystal Reports 324

## D

- Daily administration 229
- Dashboard 232
- Data retention 318
- Database
  - Changing location 296
  - Connecting to 320
  - Size 318
- Date formatting 210
- Dead Letters
  - Causes 138, 139, 162, 227, 228
- Delegating
  - Console Access 304
  - Quarantine management 304

- Spam management 304
- Delete message 168
- Delivery, email 270, 275
- Deployment scenarios 19
- DHA attacks
  - configuring attack prevention 121
  - disabling attack prevention 124
  - enabling prevention 124
  - understanding 120
- Dial-Up 281
- Digest templates 198
- Directory 298
- Directory connectors 62, 177
- disabling
  - DHA attack prevention 124
- Disclaimers. *See* Message stamps
- Distributed enterprise 25
- DMZ 24, 246
- DNS 40, 59, 61, 82, 277
- DNS blacklists 111, 158
- DoS attacks
  - configuring attack prevention 117
  - understanding 117
- Drill-down 324

## E

- eicar.com 66
- email
  - restricting incoming 117
  - securing inbound 290
  - securing outbound 291
  - securing with TLS 288
- Email batching 281
- Email content policies 97, 98
- Email headers
  - Matching 144
  - Rewriting 163

- Email history 243
- Email messages
  - Forwarding 237
  - Processing logs 238
  - Processing manually 240
  - Releasing manually 240
  - Retention 238
  - Viewing 236
- Email policy
  - Default 124
  - Understanding 127
  - Viewing and printing 173
- Email policy elements 175
- Email processing server
  - Adding or deleting 283
  - Changing array port settings 295
- Email transport policies 98
  - enabling
    - DHA attack prevention 124
- Engine, MailMarshal 8
- Enterprise installation 25
- ESMTP
  - Authentication 116, 150
  - Connection 156
  - Spoofing criterion 150
- Event Log 254
- Exporting
  - Configuration 260
  - Reports 324
  - TextCensor scripts 191
- External commands
  - Configuring 225
  - Message release 312
  - Rule action 161
  - Rule condition 143

## F

- Fallback host, email delivery 270
- False positives
  - Spam 303
  - TextCensor scripts 193
- File extension 142
- File name 142
- File type signatures, custom 140
- File types 140
- Filtering email 97
- Firewall 62, 270, 277
- Folders
  - and virus scanning 65
  - Archive 235, 236
  - Compression of 37
  - Dead Letter 228, 235
  - Default permissions 248
  - Default security 248
  - Locations 37, 297
  - Logging 37
  - Permissions 249
  - Quarantine 38
  - Queues 37
  - Searching 244
  - Security 246, 249
  - Setting up Spam Quarantine Management 307
  - Unpacking 37
  - Using 212
  - Viewing contents 235

## G

- Goto action 168

**H**

- Header Matching
  - Map Files 335
- Header matching 144
- Header rewriting
  - Map files 335
  - Order of evaluation 225
  - Rule action 163
- Headers, email
  - Altering 219
  - Deleting 223
  - Inserting 223
  - Matching 219
  - Rewriting 219
- HELO
  - incompatibility with TLS 288
- History. *See* Alert History, Email History
- HTTPS 102

**I**

- Image Analyzer 151, 337
- Importing
  - Configuration 260
  - TextCensor scripts 191
  - User Groups 298
  - Users 62
- inbound communications
  - securing with TLS 290
- Installation
  - Array 48
  - Standalone server 46, 48
- Installation options 19
- Introduction 1
- ISP 59, 60, 270, 277

**K**

- Keys, MailMarshal license
  - Entering 259
  - Invalid 258
  - Requesting 259
  - Required 257
  - Trial 56

**L**

- LDAP
  - Configuring connectors 177
  - Creating connectors 62
  - Customizing connectors 178
  - User groups 179
- License key. *See* Keys
- Licensing 257
- licensing
  - managing licenses 257
  - requesting license keys 259
  - reviewing installed licenses 258
- Load Balancing 24, 270, 283
- Local domains
  - and license keys 258
  - Configuring 56, 264
  - Delivery 286
  - Spoofing 149
  - User matching 132
- Localhost 22
- Logging
  - Classifications 163
  - Daily log files 255

**M**

- Mail Recycle Bin 235, 237, 238
- MailMarshal Today 232

Manager security 281  
managing  
    licenses 257  
    TLS keys and certificates 289  
Marshal Reporting Console 317  
McAfee for Marshal 105  
Message holding 167  
Message parking 167, 235  
Message release 312  
Message size 141, 156  
Message stamps 163, 202  
Message templates 195  
Move the message 166  
MX record 21, 61, 82, 264

## N

Node. See Email processing server  
Notification message 162  
Notifications 137, 162, 195, 225  
Number of attachments 146  
Number of recipients 144

## O

Open relay. See Anti-relaying  
Order of evaluation 164, 187, 189, 190  
outbound communications  
    securing with TLS 291

## P

Parameters  
    Message Release 313  
    Report 321  
Pass message to rule 168  
Performance Monitor 254, 255  
PestPatrol for Marshal 65, 105, 212, 340

Policy groups  
    Creating 128  
    Order of evaluation 170  
POP3 265, 278  
Ports. See TCP ports  
Postmaster. See Administrative  
    notifications  
Prerequisites 45  
preventing  
    attacks 116  
    DHA attacks 120  
    DoS attacks 117  
procedure  
    See how to  
Properties configuration 88  
Properties, MailMarshal 88  
Properties, Node 88  
Proxy settings 104  
PTR lookups 114

## Q

Quarantine 241  
Quarantine Management 303  
Queued domains 234  
Queued messages 234

## R

Receiver binding 287  
Receiver threads 287  
Receiver, MailMarshal 8  
Refuse message 169  
Regular expressions 218, 331  
Relay domain 265  
Relay server 62, 270  
Relaying  
    See *also* Anti-Relaying

- Allowing 110, 156, 157, 169
- Blocking 97
- Defined 109
- Release Message 241
- Report window 323
- Reporting groups 319
- Reports
  - Classifications 163
  - Console 93
  - Exporting 324
  - Installing 69
  - Using 317
- Reputation services 111, 158
- requesting
  - license keys 259
- Restore
  - Configuration 260
- Routing, email
  - Rule based 165
- RTF message stamping 203
- Rule actions
  - Receiver 169
  - Standard 160
- Rule conditions
  - Receiver 155
  - Standard 134
- Rule user matching 130, 131, 133
- Rules
  - Creating 129
  - Global header rewriting 218
  - Order of evaluation 170
  - Receiver 129
  - Spam Quarantine 310
  - Standard 129
- rules
  - URLCensor 100
- Rulesets. See Policy groups

## S

- Schedules
  - Folder 167
  - Policy groups 128
  - User group reload 64
- Searching
  - Email history 244
  - Folders 244
- securing
  - email communications 288
  - inbound communications 290
  - outbound communications 291
- Security
  - Console 246
  - Manager 281
- security
  - working with TLS certificates 289
- Sender ID 147, 150
- Sender, MailMarshal 8
- Sender's IP address 154, 156
- Server health 229
- Server name 286
- Server statistics 232
- Server threads 292
- Server, Email processing 282
- Set message routing 165
- Signatures. See Message stamps
- SMTP 23
- SMTP Authentication 272
- Spam 97, 98, 144, 147, 303, 310, 319
- Spam Quarantine Management 70, 94, 304
- SpamCensor 102, 135
- SpamProfiler 101, 135
- SPF 159, 170
- Spoofing 147, 148, 149, 150
- Stamp message 163
- Standalone server 20, 46, 48

Storage requirements 318  
Subject line 109, 163, 186

## T

task

See how to

TCP ports

25 20, 22

97 22

110 20

1433 69

19001 25, 232

Templates

Administrative 196

Digest 198, 307

Notification 162, 196

Terminal actions 159, 166, 167, 168

TextCensor scripts

Editing 187

Operators 187

Rule condition 142

Special characters 186

Syntax 190

Testing 194

Understanding 184

Weighting 188

Third 337

Timeouts, email delivery 293

TLS

description 288

HELO incompatibility 288

limitations 288

working with certificates 289

TLS Certificate Wizard

creating and managing certificates  
and keys 290

supported operations 289

Tools, MailMarshal 95

## U

UDP 59, 277

Understanding 85, 127, 175

Uninstalling MailMarshal 81

Upgrading MailMarshal 76

URLCensor 100

User groups 179–184

Reloading 180

User Matching. See Rule User Matching

Users 183

Users, importing 62

## V

Valid fingerprints 140, 165

Variables 161, 170, 197, 201, 203, 204,  
210, 213

Virus cleaning 136, 138

Virus scanners

Appliance 65

Configuring 105

Installing and configuring 65

Results 136

Rule condition 136

Virus scanning 97

Viruses 105

## W

Web Console 70, 92

Wildcards 190, 329

Windows event logs

Filters 251

