M86 MailMarshal SPE

ADMINISTRATOR GUIDE

Software Version: 3.0.1

M86 MAILMARSHAL SPE ADMINISTRATOR GUIDE

Published August 2010 for software release 3.0.1

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.

Contents

Chapter 1

Chapter 2

Chapter 6

Chapter 7
Understanding Email Policy, Policy Groups, and Rules 163

Appendix A
Wildcards and Regular Expressions 233

Glossary 241

Index 247

About This Book and the Library

The *Administrator Guide* provides conceptual information about MailMarshal SPE. This book defines terminology and concepts.

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Administrator Guide
: Provides conceptual information and detailed planning and installation information about MailMarshal SPE for service providers. This book also provides an overview of the MailMarshal SPE user interfaces and the Help.

User Guide
: Provides administration and configuration information for customers subscribing to an email content security managed service that uses MailMarshal SPE. M86 Security provides this document in generic format, ready to be customized and branded by the service provider.

MailMarshal SMTP User Guide
: Provides installation, administration, and configuration information about the email server infrastructure of MailMarshal SMTP. Note that not all features of MailMarshal SMTP are available in MailMarshal SPE.

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
Bold	- *Window and menu items* - *Technical terms, when introduced*
Italics	- *Book and CD-ROM titles* - *Variable names and values* - *Emphasized words*
`Fixed Font`	- *File and folder names* - *Commands and code examples* - *Text you must type* - *Text (output) displayed in the command-line interface*
Brackets, such as [*value*]	- *Optional parameters of a command*
Braces, such as {*value*}	- *Required parameters of a command*
Logical OR, such as *value1*|*value2*	- *Exclusive parameters. Choose one parameter.*

DEFINITIONS

The library uses consistent naming conventions to identify the components of the products described and user roles. The following table summarizes these conventions.

Term	Definition
MailMarshal SPE	MailMarshal Service Provider Edition: The M86 Security product designed to manage multiple arrays of MailMarshal SMTP Servers, to deliver email content security in a Service Provider environment.
MailMarshal SMTP	The M86 Security gateway email content security server solution. Processes email at the network gateway to protect against spam, viruses, gateway email attacks, and other undesirable consequences of using email.
Service Provider	An organization that provides managed email content security and other Internet services for customer organizations, from a centralized location.
Service Provider Administrator	The personnel who manage application configuration and site-wide settings for the Service Provider
Customer	An organization that subscribes to the email content security service delivered by the Service Provider.
Advanced Customer	An organization that subscribes to advanced features of the service.
Customer Administrator	The personnel who manage local configuration and email content security settings for the Customer organization.
User	Any individual email user within the Customer organization.

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.

Email content security has traditionally required specialized software to be installed at the gateway to each organization’s site. Bandwidth considerations and the growing complexities of content security issues have led to substantial ongoing costs related to installation, upgrading and management of the software.

WHAT IS MAILMARSHAL SPE?

MailMarshal SPE is an email content security application for organizations, designed to be hosted at the data center of a Service or Solution Provider. MailMarshal SPE leverages the power of award-winning gateway email content security solution MailMarshal SMTP, for use in a managed service environment. Through MailMarshal SPE, the complexity and cost of email content security for the user organization can be notably reduced.

MailMarshal SPE allows the Service Provider to manage email content security for customers from a single centralized interface. The Administration Web Console is a web-based interface that can manage MailMarshal SMTP servers, rules, messages, reports, audits and customers.

MailMarshal SPE also offers configurable functionality for customer organizations that have subscribed to advanced options. The Customer Web Console allows customer administrators to adjust the settings of MailMarshal components such as the URLCensor and TextCensor. Customer organizations can filter messages based on their own requirements.

MailMarshal SPE works seamlessly with customers’ internal email systems. All content email content security management, spam protection, and Acceptable Use Policy enforcement actions occur transparently at the Service Provider gateway. Customers and Users will benefit with a transparent, safe, secure, and productive email environment.

Note: *For definitions of the terms used in this document to describe organizations and MailMarshal SPE components, see “Definitions” on page xiii.*

WHAT DOES MAILMARSHAL SPE PROVIDE?

MailMarshal SPE provides a framework that allows a Service Provider to deliver managed email content security services for other organizations. Email processing tasks are performed by a number of MailMarshal SMTP servers located within the Service Provider’s network.

With MailMarshal SPE, the Service Provider can dynamically allocate MailMarshal SMTP Servers to a particular Customer organization as an email content security service. All policy elements, including enforcing Acceptable Use Policy and protecting against spam, viruses and other undesirable content, can be managed remotely by the Service Provider and the Customer using Web-based consoles. Email processing efficiency is as efficient for the customer as with an on-site MailMarshal SMTP deployment.

MailMarshal SPE provides web based interfaces to meet the needs of Service Provider and customer administrators and users (email recipients). These include:

Administration Web Console:

Allows the Service Provider Administrator(s) to monitor and manage Customers, review MailMarshal SMTP server information, and establish preset policies for Customers.

Customer Web Console:

Allows the Customer Administrator(s) to monitor and control product activity for their respective organizations. Customers who have advanced subscriptions can establish their own email policies

Customer SQM Console

Hosted with the Customer Web Console, the SQM allows users to manage messages quarantined as spam (or for other reasons).

MailMarshal SPE provides total administrative control of all underlying MailMarshal SMTP Servers. The product provides Service Provider Administrators with granular control of policies, and the ability to delegate email monitoring and control to other email Administrators. Further customizations can be achieved by allowing Customer Administrators to configure email policies.

MailMarshal SPE provides the ability to manage arrays of MailMarshal SMTP Array Managers. This function delivers a Service Provider architecture that is scalable to large numbers of customers. MailMarshal SPE is designed to deliver email content security services for very large user numbers and very large volumes of email.

HOW MAILMARSHAL SPE WORKS

MailMarshal SMTP is a server-based Simple Mail Transfer Protocol (SMTP) email content scanning product. MailMarshal SPE uses one or more MailMarshal SMTP Servers as email gateways to enforce email content security policies for customer organizations. All configuration of the gateway for delivery and scanning rules is provided through MailMarshal SPE.

Understanding What MailMarshal SMTP Does

The MailMarshal SMTP server functions as an email gateway. All inbound and outbound email passes through MailMarshal SMTP.

Each MailMarshal Server runs several component services, including the Receiver, Engine, and Sender services. Email enters the MailMarshal Server at the Receiver, where MailMarshal SMTP applies any enabled Receiver rules. Receiver rules offer powerful protection because they can 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 by splitting it into header, and message, and expanding any attached archive or compressed files. The Engine then checks each component against the email policy (rules) you have enabled, including SpamCensor scripts, URLCensor, 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 by running antivirus scanning software. MailMarshal SMTP directly supports special high-throughput DLL interfaces to several scanners. For details of supported scanners, see M86 Knowledge Base article Q10923.

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.
- Email that triggers rules can be copied or quarantined, among other actions.

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.

Monitoring and Reporting

The MailMarshal SPE Administrator Console and Customer Console provide a number of features that allow Service Provider and Customer Administrators to review and report on MailMarshal activity.

The Administrators can delegate access to other users for specific Console functions or specific quarantine folders.

MailMarshal SPE Support for MailMarshal SMTP Features

MailMarshal SPE provides access to most, but not all, features of MailMarshal SMTP. Supported features are documented in this Guide. If you have questions about features not documented here, contact M86 Security for information.

What's New In This Version?

MailMarshal SPE 3.0 introduces a number of enhancements, and support for additional MailMarshal SMTP features. Items added include:

Marshal IP Reputation Service
A DNS based lookup service maintained by M86 Security.

Blended Threats Module
A database of malicious URLS for message body checking, maintained by M86 Security.

New Customer Console
The Customer Console has been updated in look and performance. The Customer Console can be installed on more than one server.

MailMarshal SMTP 6.8 Support
MailMarshal SPE 3.0 works with MailMarshal SMTP 6.8.3 and supports most functionality (including new rule conditions and actions, and global settings) found in this version of MailMarshal SMTP.

For full details of new and updated items, see the Release Notes.

Chapter 2
Planning Your MailMarshal SPE Installation

When planning to install MailMarshal SPE, you should understand how MailMarshal SPE manages various architectures of the MailMarshal SMTP Array Managers and Servers, 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

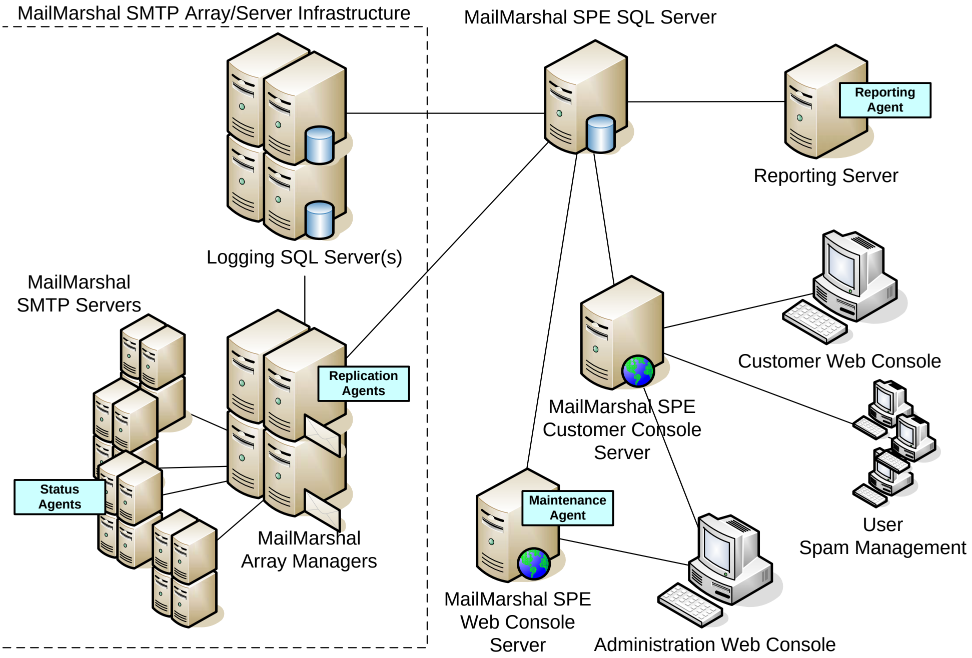
Plan your MailMarshal SPE installation by reading the following sections and completing the following checklist:

☑	**Step**	**See Section**
□	**1.** Learn about important MailMarshal SPE concepts.	“Understanding MailMarshal SPE Components” on page 9 and “Understanding Email Flow in MailMarshal SPE” on page 12.
□	**2.** Choose the appropriate architecture for your service provider environment.	“MailMarshal SPE Architecture” on page 16
□	**3.** Determine the number and location for the MailMarshal SMTP Array Managers and Servers that perform the email processing.	“MailMarshal SPE Architecture” on page 16

☑	Step	See Section
□	**4.** Ensure the architecture provides the necessary processing power, and computers meet the hardware and software requirements.	“MailMarshal SPE Architecture” on page 16
□	**5.** Determine the supporting database server architecture.	“MailMarshal SPE Architecture” on page 16 and “Database Server Considerations” on page 30.
□	**6.** Create the appropriate Service Provider branding customizations.	“Configuring Service Provider Branding” on page 50
□	**7.** Collect installation information about your Service Provider environment.	“Collecting Information for Installation” on page 34.

UNDERSTANDING MAILMARSHAL SPE COMPONENTS

MailMarshal SPE 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 various deployment requirements of the Service Provider. The MailMarshal SPE components are shown on separate computers in the following figure. As a minimum, you can install the components on a single computer, with the SPE SQL Server run on a separate machine


MailMarshal SMTP Array/Server Infrastructure
MailMarshal SPE SQL Server
Reporting Agent
Reporting Server
Logging SQL Server(s)
MailMarshal SMTP Servers
Replication Agents
Status Agents
MailMarshal Array Managers
Customer Web Console
MailMarshal SPE Customer Console Server
User Spam Management
Maintenance Agent
MailMarshal SPE Web Console Server
Administration Web Console

MailMarshal SMTP Components

MailMarshal SPE includes the following components:

Administration Web Console

Web-based console that allows Service Provider Administrators to manage and monitor customer information, configure system wide policies, and control global MailMarshal SMTP settings.

Web Console Server

Provides website services for the Web Console. The Web Console must be installed on a server with Microsoft IIS 6.0 or above installed, including the Active Server Pages component.

Customer Web Console and SQM

Web-based console that allows Customer Administrators to define organization users and email policy (rules), and configure additional email gateway settings. The Spam Quarantine Management (SQM) web application allows customer users to self-manage quarantined messages.

Customer Console Server

Provides website services for the Customer Web Console and SQM application. The Web Console must be installed on a server with Microsoft IIS 6.0 or above installed, including the Active Server Pages component.

Reporting Server

Used to prepare pre-existing scheduled reports and emails selected reports to Administrators and end users.

SPE SQL Server

Stores data and configuration information for MailMarshal SPE. For more information, see “MailMarshal SPE Architecture” on page 16.

MailMarshal SPE Agent Services are essential run-time components used to carry out management tasks as configured by Service Provider and customer Administrators. To operate properly, MailMarshal SPE requires MailMarshal SMTP Array/Server infrastructure. The Replication Agent and Status Agent must be installed on each Array Manager and SMTP Server respectively. The product installer allows you to select a server role and installs the appropriate services for that role.

Maintenance Agent

Provides performance optimization and manages temporary data retention for the Web Console server and the database. This agent must always be running and is installed on the same server as the web console.

Replication Agent

A Replication Agent is installed on every MailMarshal Array Manager that is managed by MailMarshal SPE. The Agent provides integration between MailMarshal SPE and the Array Managers, including policy updates.

Status Agent

A Status Agent is installed on each MailMarshal SMTP Server that is managed by MailMarshal SPE. The Agent supplies real-time notifications about the servers' conditions to MailMarshal SPE.

Reporting Agent

Performs regular data mining and reporting functions from the SPE SQL Server. The Agent can be installed in a variety of locations. For details, see page 19.

Other Software and Services

Logging SQL Server

MailMarshal SPE retrieves data about each MailMarshal SMTP Array from the respective Logging databases. This typically includes message logging and configuration of each Array.

Connector Agent

Allows LDAP and/or Active Directory user groups to be synchronized from a customer's environment to the SPE server, using HTTP or HTTPS.

Array Manager

Manages an array of MailMarshal SMTP email processing servers. The Array Manager connects to the email processing servers and to the Logging database, hosted using Microsoft SQL Server.

MailMarshal SMTP Email Processing Server

Accepts email, applies policy in the form of rules, and forwards email to the appropriate internal or external recipient.

UNDERSTANDING EMAIL FLOW IN MAILMARSHAL SPE

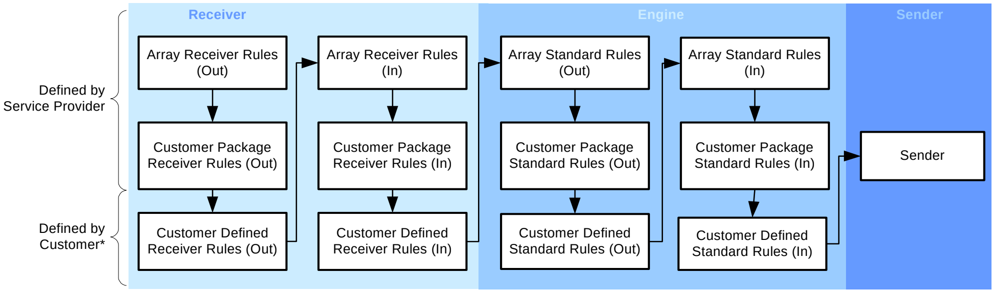
MailMarshal SPE provides a single access point that allows a service provider to configure, control and report email flows for multiple organizations. Email flow in MailMarshal SPE is largely identical to the flow in MailMarshal SMTP. However with MailMarshal SPE, the processing and logging of email for several organizations is carried out on a shared array of email processing servers.

MailMarshal SPE allows each subscribing organization to assess and enforce its own company email Acceptable Use Policy, manage client use of bandwidth, prevent confidential information from leaving the company, and increase employee productivity. Working transparently to all users, MailMarshal SPE works at the Service Provider gateway, filtering and removing dangerous and undesirable objects before they can enter the organization's network.

MailMarshal SPE allows email processing rules to be managed at three levels.

1. The Service Provider can apply array policies to one or more arrays in the infrastructure.
2. The Service Provider can create policy packages for customers. Packages can be mandatory or optional for customers.
3. Each Advanced customer organization can configure rules. Customer-defined Rules allow each customer the flexibility to match and enforce its own Acceptable Use Policy. For example, the rules can check for inappropriate content, confidential material, specific keywords, and other criteria important to the organization. Customer defined rules can be offered as a value-added option on a subscription plan.

To better explain how MailMarshal SPE manages email for multiple organizations and to help plan your MailMarshal SPE installation, the following sections describe how MailMarshal SPE controls inbound and outbound email flows.


Defined by Service Provider
Defined by Customer*
Receiver
Engine
Sender
Array Receiver Rules (Out)
Customer Package Receiver Rules (Out)
Customer Defined Receiver Rules (Out)
Array Receiver Rules (In)
Customer Package Receiver Rules (In)
Customer Defined Receiver Rules (In)
Array Standard Rules (Out)
Customer Package Standard Rules (Out)
Customer Defined Standard Rules (Out)
Array Standard Rules (In)
Customer Package Standard Rules (In)
Customer Defined Standard Rules (In)
Sender

* Availability of Customer Package Rules and Customer Defined Rules depends on subscription options set by the Service Provider.

Inbound Email Flow

Each organization's inbound email at the internet gateway is directed to a pre-assigned array of MailMarshal SMTP email processing servers (using MX records or other routing methods). For more information on assigning processing resources to clients, please see “MailMarshal SPE Architecture” on page 16 and “Configuring Customers” on page 75.

Once email has been received, the processing flow is identical for all customer organizations. First, connections and messages are validated against MailMarshal SMTP Receiver rules. Receiver rules can reject email based on various criteria. For example, the Denial of Service (DoS) receiver rules handle a deluge of SMTP requests that can result in system overload to protect the system from this type of attack. SpamProfiler can block a significant portion of spam at the receiver. Receiver policies and rules help cull much undesirable email before it enters your network. None of this traffic enters the network, so MailMarshal SPE does not log this activity.

If an email is not blocked by a Receiver rule, the MailMarshal server copies the email to a working folder. The MailMarshal Engine component splits the email into header, message, and attachment components. If necessary, the Engine recursively uncompresses any attachments to analyze the original files.

MailMarshal can apply a number of filtering mechanisms to identify viruses, spam (SpamCensor, SpambotCensor, SpamProfiler), undesirable URLs embedded in the email (URLCensor and Blended Threat Module), specific text (TextCensor), country of origin (CountryCensor), and other content. The identified items can be excluded, flagged, or logged. Rules can block email based on attachment size, unapproved relaying, sender or recipient, inclusion on unapproved lists, such as DNS, Phishing, or URL blacklists, and many more characteristics.

The rules can direct MailMarshal to take specified actions based the rule results. For example, if an email contains a virus, MailMarshal quarantines it. If the message is acceptable but the attachment is not, MailMarshal can strip the attachment but deliver the message, and notify the recipient of its actions.

If the email is virus-free and not flagged by any other rules, MailMarshal SMTP deletes the copy of the email from the working folder and delivers the original message to the MailMarshal Sender. Optionally, the service provider can enforce Global and Array level rules just before the final delivery to the Sender. For example, messages can be stamped with the Service Provider's name and support number. Upon final acceptance, the Sender delivers the message to the customer organization’s email server for delivery.

If the message does trigger a rule, MailMarshal SMTP quarantines the message, notifies the recipient, and logs the event. MailMarshal SMTP can also take additional actions such as to notify an Administrator, strip attachments, quarantine messages, classify messages, or conditionally deliver messages based on group membership. For example, a customer Administrator can configure rules to deliver email with image file attachments to the Marketing group but not to the Help desk group.

Outbound Email Flow

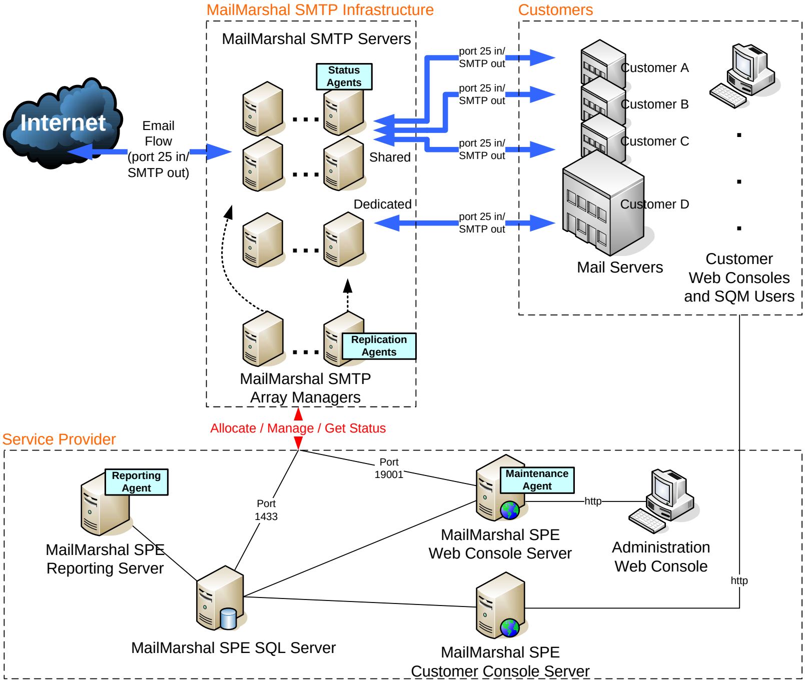
MailMarshal SPE handles outbound email flow in a similar way to inbound email flow. An organization’s internal email server sends email to the service provider’s email infrastructure. Messages are routed to a designated array of MailMarshal SMTP Servers for processing. The MailMarshal Receiver inspects each message, and then places a copy of the email in a working folder. The MailMarshal Engine splits the email into the header, message body, and any attachments to analyze using the Outbound rules. If the email components pass all rules (including those from the Service Provider at Global and Array levels), the MailMarshal Sender queues or forwards the message for delivery. If the email triggers a rule, MailMarshal SPE processes the email as specified by the rule action.

MAILMARSHAL SPE ARCHITECTURE

The architecture of MailMarshal SPE is summarized in the figure below. MailMarshal SMTP Servers can be installed on a number of computers to create one or more arrays of email processing servers in a Demilitarized Zone (DMZ). The MailMarshal SMTP servers will receive inbound email on port 25, process it, and forwards it for delivery to the customer mail servers. Similarly for outbound SMTP traffic, MailMarshal SMTP servers will process all outgoing emails from the customers.

An array of MailMarshal SMTP email processing servers can be used to process email for several small to medium-sized organizations. The assignment of arrays to customers is performed from the Administration Web Console. You can add more email processing power for large enterprises by dedicating a whole array of email processing servers to a single customer.

To cater for larger and increasing email volumes, the underlying MailMarshal SMTP Array/Server infrastructure provides a broad range of enterprise configurations that can include redundancy and failover support over. For more information about MailMarshal arrays, please refer to “Array Installation” in the *MailMarshal SMTP User Guide*.


MailMarshal SMTP Infrastructure
MailMarshal SMTP Servers
Status Agents
Internet
Email Flow (port 25 in/ SMTP out)
Shared
Dedicated
Replication Agents
MailMarshal SMTP Array Managers
port 25 in/ SMTP out
port 25 in/ SMTP out
port 25 in/ SMTP out
port 25 in/ SMTP out
Customers
Customer A
Customer B
Customer C
Customer D
Mail Servers
Customer Web Consoles and SQM Users
Allocate / Manage / Get Status
Service Provider
Reporting Agent
MailMarshal SPE Reporting Server
Port 1433
Port 19001
Maintenance Agent
http
MailMarshal SPE Web Console Server
Administration Web Console
http
MailMarshal SPE SQL Server
MailMarshal SPE Customer Console Server

***Note:** For any infrastructure configuration, it is essential to install Replication Agent and Status Agent on each Array Manager and SMTP Server respectively.*

To cater for increased numbers of customers, MailMarshal SPE is designed to scale up and out, by supporting both multi-processor and multi machine configurations. MailMarshal SPE is also designed to work with geographically separated servers.

The Service Provider aspects to consider for scalability are:

- MailMarshal SPE Web Console Server
- MailMarshal SPE Customer Console Server
- MailMarshal SPE SQL Server
- MailMarshal SPE Reporting Server

The **MailMarshal SPE Web Console Server** hosts the Administration Web Console using Microsoft IIS Web server(s).

The **MailMarshal SPE Customer Console Server** hosts the Customer Web Console and Spam Quarantine Management thin clients using Microsoft IIS Web server(s). To handle increasing HTTP requests, you can install multiple servers and/or load balancing software to manage peak traffic to the website.

The **MailMarshal SPE SQL Server** stores data and configuration information for MailMarshal SPE. This SQL Server supports use of a number of cluster techniques offered by Microsoft SQL Server: High Availability, Load-balancing, and High-performance clusters.

The **MailMarshal SPE Reporting Agent** gathers data from MailMarshal SPE SQL Server, and performs data processing. The install location of the Reporting Agent does not affect email processing performance, but it can affect the performance of the MailMarshal SPE SQL Server. For best results, install Reporting Agent in one of the following locations, depending on your preference:

- To consolidate CPU processing resource, install Reporting Agent on the same server as the MailMarshal SPE Customer Console Server. Since Reporting Server performs scheduled reports and emailing operations in bursts, installing the Reporting Server on the computer that hosts Microsoft IIS results in saving of unused processing resources.
- To allow efficient interaction between the database and reporting, install Reporting Agent on the same server as the SQL database server for direct communication. Ensure this server has the capacity to run these two services.
- For portability, install Reporting Agent on another computer in the network close to the computer hosting the database. Ensure that these servers have a high-speed network connection.

Recommended Software Configuration

The following table indicates which processing roles can share servers in production environments:

Server Role	Shared Server	Dedicated Server
SQL Server	✗	✓
Admin Console (IIS Server)	✓	✓
Customer Console (IIS Server)	✓	✓
Reporting Server	✓	✓

Server Role	Shared Server	Dedicated Server
Array Manager	✓	✓
SMTP Email Processing Server	✓	✓
Domain Controller	✗	✓

MailMarshal SPE with one server

It is possible to install all of the components of MailMarshal SPE on a single server. This scenario is not recommended for a production environment, but it is useful to test or demonstrate an installation.

MailMarshal SPE with two servers

The table below shows the recommended installation using two servers. External facing functions are installed on Server 2. The MailMarshal SMTP Array Manager and Processing Node are separated to enhance performance.

Server Role	Server 1	Server 2
SQL Server	✓	
Web Console (IIS Server)	✓	
Customer Console (IIS Server)		✓
Reporting Server	✓	
Array Manager	✓	
SMTP Email Processing Server		✓

MailMarshal SPE with three servers

The table below shows the recommended installation using three servers:

Server Role	Server 1	Server 2	Server 3
SQL Server	✓		
Web Console (IIS Server)		✓	
Customer Console (IIS Server)			✓
Reporting Server	✓		
Array Manager		✓	
SMTP Email Processing Server			✓

MailMarshal SPE with four servers

The table below shows the recommended installation using four servers. Two Processing Nodes are installed.

Server Role	Server 1	Server 2	Server 3	Server 4
SQL Server	✓			
Web Console (IIS Server)		✓		
Customer Console (IIS Server)			✓	

Server Role	Server 1	Server 2	Server 3	Server 4
Reporting Server	✓			
Array Manager		✓		
SMTP Email Processing Server			✓	✓

HARDWARE AND SOFTWARE REQUIREMENTS

The following sections specify the recommended hardware and software for various computers where you may be installing MailMarshal SPE components. Consider all the requirements before mapping your MailMarshal SPE installation.

MailMarshal SMTP Installation Requirements

To enable MailMarshal SPE to access the MailMarshal SMTP databases, in MailMarshal SMTP you must specify the database server location using a name or address that can be resolved externally to the local computer. You *cannot* specify the database server location using a loopback address. For example, you cannot use the values `localhost` or `127.0.0.1` even if the MailMarshal SMTP database is located on the same computer as the Array Manager. Instead specify the server with an IP address such as `192.168.1.1` or a server name such as `MMServer`.

Web Console Installation Requirements

The following table lists system requirements for Web Console Server and its Maintenance Agent companion. The minimum hardware requirements are based on an estimate of 100,000 page hits per day.

Category	**Requirements**
Processor	**Minimum**: Dual core processor
Disk Space	**Minimum**: 20GB (NTFS)
Memory	**Minimum**: 1GB *(2GB for 64 bit systems)*
Supported Operating System	• *Windows Server 2008 SP2 (32 or 64 bit edition) or Server 2008 R2* • *Windows Server Standard or Enterprise 2003 SP2*
Network Access	• *TCP/IP protocol* • *Domain structure* • *External DNS name resolution - DNS MX record to allow access from other computers in the MailMarshal installation* • *DNS resolution - IP lookup facility to send message notifications* • *If installed with IIS 6.0: host header address with port 80 for website domain*
Software	• *Microsoft Internet Information Services (IIS) 6.0 or later, including Active Server pages option* • *For IIS 7.X role service requirements, see M86 Knowledge Base article Q13814.* • *Microsoft .NET Framework 3.5 SP1 or later*

Category	Requirements
Port Access	• *Port 25 - to the SMTP server specified in global configuration, for administrative email notifications and message releasing from the Web Console* • *Port 80 (HTTP) and Port 443 (HTTPS) inbound - for website requests* • *Port 1433 - for connection to SQL Server database*
SSL Certificate	• *If you want to configure the Web Console Server for HTTPS, use a valid certificate signed by a trusted authority*

MailMarshal SPE SQL Database Installation Requirements

The following table lists system requirements for the SQL Server system to be used with MailMarshal SPE

Category	Requirements
Processor	Current generation processor (Microsoft recommends 2GHz or better for SQL Server 2008 Standard)
Disk Space	**Minimum**: 10GB (NTFS)
Memory	**Minimum**: 2GB
Supported Operating System	• *Windows Server 2008 SP2 (32 or 64 bit edition) or Server 2008 R2* • *Windows Server Standard or Enterprise 2003 SP2*
Network Access	• *TCP/IP protocol* • *Domain structure* • *DNS service available*

Category	Requirements
Software	• *SQL Server 2005* ***SP3*** • *SQL Server 2008* ***SP1*** • *SQL Express is NOT supported.*
Port Access	• *Port 1433 - for inbound connection to SQL Server database*

Note: *There are further options to cluster database servers. Please see "Database Server Considerations" on page 30.*

Agent Services Installation Requirements

Agent services are the components that connect the MailMarshal SMTP services into a MailMarshal SPE installation.

In Agent Services installations, computer requirements for the components may vary depending on whether a single server or separate servers are used for Array Manager and MailMarshal SMTP email processing servers. Furthermore, computer requirements can also vary depending on the location of the MailMarshal SPE Reporting Server.

Note: *Minimum prerequisites are greater than the base prerequisites for MailMarshal SMTP servers. At this writing MailMarshal SPE is only compatible with MailMarshal SMTP version 6.8.3.*

Replication Agent service

The following table shows the updated *minimum* requirements for a MailMarshal SMTP Array Manager server with Replication Agent installed:

Category	Requirements
Processor	Dual core processor
Disk Space	**Minimum**: 10GB (NTFS)

Category	**Requirements**
Memory	**Minimum**: 1GB *(2GB for 64 bit systems)*
Supported Operating System	• *Windows Server 2008 SP2 (32 or 64 bit edition) or Server 2008 R2* • *Windows Server Standard or Enterprise 2003 SP2*
Network Access	• *TCP/IP protocol* • *Domain structure* • *DNS service available*
Software	• *Database server: SQL Server 2005* ***SP3*** *or SQL Server 2008* ***SP1****. SQL Express is NOT supported. For more information about database considerations, see “Database Server Considerations” on page 30.* • *Microsoft .NET Framework 3.5 SP1* • *MailMarshal SMTP (6.8.3 only)* • *Antivirus scanning software supported by MailMarshal SMTP. For more information, see M86 Knowledge Base article Q10923.*
Port Access	• *Port 25 - to the SMTP server specified in Global Configuration, or in the array settings, for email notifications* • *Port 53 - DNS external email server name resolution* • *Port 80 (HTTP) and Port 443 (HTTPS) - SpamCensor updates* • *Port 1433 - Communication with MailMarshal SPE SQL Server database* • *Port 19001 - Communication with MailMarshal SMTP Array Manager in trusted network*

Status Agent service

The following table shows the updated requirements for a MailMarshal SMTP Server with Status Agent installed.:

Category	Requirements
Processor	**Minimum**: Dual core processor
Disk Space	**Minimum**: 10GB (NTFS)
Memory	**Minimum**: 1GB (2GB preferred)
Supported Operating System	• *Windows Server 2008 SP2 (32 or 64 bit edition) or Server 2008 R2* • *Windows Server Standard or Enterprise 2003 SP2*
Network Access	• *TCP/IP protocol* • *Domain structure* • *DNS service available*
Software	• *Antivirus scanning software supported by MailMarshal SMTP* • *Microsoft .NET Framework 3.5 SP1 or later* • *MailMarshal SMTP (6.8.3 only)*
Port Access	• *Port 25 - to the SMTP server specified in Global Configuration, or in the array settings, for email notifications* • *Port 53 - DNS external email server name resolution* • *Port 80 (HTTP) and Port 443 (HTTPS) - SpamCensor updates* • *Port 1433 - Communication with MailMarshal SPE SQL Server database* • *Port 19001 - Communication with MailMarshal SMTP Array Manager in trusted network*

Reporting Agent

The following table shows the requirements for Reporting Agent running on a dedicated computer. If you install either MailMarshal SPE Database server or Web Console server on the same machine, the minimum hardware requirements may be greater than those shown in the table, depending on the number of users and typical volume of web requests.

Category	**Requirements**
Processor	**Minimum**: Dual core processor
Disk Space	**Minimum**: 10GB (NTFS)
Memory	**Minimum**: 1GB *(2GB for 64 bit systems)*
Supported Operating System	• *Windows Server 2008 SP2 (32 or 64 bit edition) or Server 2008 R2* • *Windows Server Standard or Enterprise 2003 SP2*
Network Access	• *TCP/IP protocol* • *Domain structure* • *DNS service available*
Software	• *Microsoft .NET Framework 3.5 SP1 or later*
Port Access	• *Port 25 - to the SMTP server specified in Global Configuration, for email delivery of reports* • *Port 1433 - Communication with MailMarshal SPE SQL Server database*

Connector Agent

The Connector Agent is installed at Customer sites. This Agent does not have large resource requirements. The server requirements below specify a normal recent workstation. The main requirements for this agent are the LDAP and HTTP communication ports.

Category	**Requirements**
Processor	**Minimum**: Dual core processor
Disk Space	**Minimum**: 10GB (NTFS)
Memory	**Minimum**: 1GB
Supported Operating System	• *Windows Server 2008 SP2 (32 or 64 bit edition) or Server 2008 R2* • *Windows Server Standard or Enterprise 2003 with Service Pack 2* • *Windows 7* • *Windows XP with Service Pack 2*
Network Access	• *TCP/IP protocol* • *Domain structure* • *DNS service available* • *Access to LDAP and/or Active Directory servers*
Port Access	• *Port 389 or other LDAP port - Communication with internal LDAP server* • *Port 80 outbound - Communication with MailMarshal SPE Web Console server* • *Port 443 outbound - Communication with MailMarshal SPE Web Console server (if the Web Console Server is configured for HTTPS)*
SSL Certificate	• *If you want the Connector Agent to communicate with the Web Console Server using HTTPS, install a valid certificate signed by a trusted authority on the Web Console server*

DATABASE SERVER CONSIDERATIONS

To estimate the redundancy and performance efficiency of MailMarshal SPE Database server and determine the total computers required for Microsoft SQL Server, review the following sample work sheet and complete My Worksheet with an appropriate server plan. If your total MB for the retention period is above 8GB, then you should consider clustering your database servers.

Notes: If the MailMarshal SPE and MailMarshal SMTP databases are hosted on separate servers, DTC must be enabled on all database servers.

- SQL Express is NOT supported for production use for the MailMarshal SPE or MailMarshal SMTP database server.

Sample Worksheet		
Number of users	=	100
Average number of valid and quarantined email messages per user per day	x	70
Average number of reports generated each hour	x	
Number of MailMarshal SMTP Array Managers	x	
Number of MailMarshal SMTP email processing servers	x	
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.

My Worksheet		
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	
Average number of reports generated each hour	x	
Number of MailMarshal SMTP Array Managers	x	
Number of MailMarshal SMTP email processing servers	x	
Safety margin	x	
Total database size in bytes for retention period	=	
Total database size in MB for retention period (divide by 1024)	=	

CONFIGURING FIREWALL SETTINGS

MailMarshal components communicate using a number of server ports. The following table provides a basic list of ports required for the various components

Port	Type	Direction	Description	Server and Component
1433*	TCP	In/Out	Microsoft SQL Server	• *MM SMTP Array Manager* • *MM SMTP Email Processing Server* • *MM SPE Web Console Servers (Admin and Customer)* • *MM SPE Database Server* • *MM SPE Reporting Agent*
25	TCP	In/Out	SMTP (Email flow and notifications)	• *MM SMTP Email Processing Servers*
25	TCP	Out	SMTP (notifications and scheduled reports)	• *MM SPE Reporting Agent* • *MM SPE Admin Web Console Server*
80	TCP	In	HTTP (Web console, Connector Agent)	• *MM SPE Web Console Servers (Admin and Customer)*
443	TCP	In	HTTPS (Web console secure, Connector Agent secure)	• *MM SPE Web Console Servers (Admin and Customer)*
80	TCP	Out	HTTP (SpamCensor updates, SpamProfiler updates)	• *MM SMTP Array Manager* • *MM SMTP Email Processing Servers*

Port	**Type**	**Direction**	**Description**	**Server and Component**
443	TCP	Out	HTTPS (SpamCensor updates)	• *MM SMTP Array Manager*
19001**	TCP	In	MailMarshal SMTP node communication	• *MM SMTP Array Manager*
19001**	TCP	Out	MailMarshal SMTP node communication	• *MM SMTP Array Manager* • *MM SPE Admin Web Console Server*
53	TCP UDP	Out	DNS server name resolution for email sending and DNS Blacklist services	• *MM SMTP Email Processing Servers*

*SQL Server port usage can be configured for other ports. 1433 is the default.
**MailMarshal SMTP can be configured to use other ports. When all MailMarshal SMTP components are installed on a single server, email processing services use port 19002 by default.

COLLECTING INFORMATION FOR INSTALLATION

Before you install the MailMarshal SMTP Array Manager and Email Processing Server infrastructure and MailMarshal SPE, you may want to collect the following information about your environment. When you run the Administration Web Console for the first time, having the following details handy can help you quickly configure MailMarshal SPE.

Information required	**My information**
Names and locations of computers in the MailMarshal SMTP Array/Servers infrastructure.	
Names of computers where you plan to install MailMarshal SPE components, including Web Console Servers, SQL Database Servers, and Reporting Servers.	
Prerequisite software for each computer where you will install software and the best time to restart each system, if necessary.	
Company name for MailMarshal SPE license.	
Website domain of your MailMarshal SPE Service Provider.	
IP address, access port, and administrative logon credentials for your Microsoft SQL server computer.	
MailMarshal SPE Administrator contact information. This includes the email address where MailMarshal SPE will send general Administrator notification emails.	

Information required	My information
IT or Support Department email addresses for more specific MailMarshal SPE notifications such as Message Queue information and Rule Errors.	
Email address that email notifications to recipients will be delivered from (reply to address).	
SMTP server IP address, primary and optional secondary DNS servers MailMarshal SPE will use for notifications.	
IP address and logon credentials for your directory server (Active Directory or LDAP).	
Server name, fully qualified domain name, or IP address of the proxy that MailMarshal uses to connect to the network.	
Email address email notifications to recipients will be from (reply to address) (can be new account).	
Security plan on minimum password lengths, and IP address ranges to grant/deny access to the Administration Web Console.	
List of users and their corresponding credentials that will be allowed access to the Administration Web Console.	
HTML branding banner for the top pane for both the Administration Web Console and Customer Web Console	

Chapter 3

Installing and Configuring MailMarshal SPE

Before you install MailMarshal SPE, be sure to complete the steps in the planning checklist. For more information, see “Planning Checklist” on page 7.

When you complete the planning checklist, you should know details of MailMarshal SMTP Servers and Array Managers that provide email processing for your MailMarshal SPE system. In addition, you should plan which database service architecture you want to install, and determine the computers you will use for each MailMarshal SPE component. Collect the information listed in “Collecting Information for Installation” on page 34 before you install components.

MailMarshal SPE provides a single installer that you can use to install one or more of the product components at a time. The instructions below assume that each component is installed separately. To install more than one component, on the Server Roles window of the installer select **Custom/Complete**, and then use the Select Features window to select components to install.

Note: *It is possible to install all MailMarshal SPE components, including the Web Consoles, Reporting Server, MailMarshal SMTP Server, Array Manager, and databases, on one computer. This configuration is not recommended for production environments but may be useful for demonstration purposes. For more information about MailMarshal SPE environments, see “MailMarshal SPE Architecture” on page 16 and “Hardware and Software Requirements” on page 22.*

INSTALLATION CHECKLIST

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

☑	**Steps**	**See Section**
□	**1.** Install prerequisite software	"Installing Prerequisite Software" on page 39.
□	**2.** Install MailMarshal SMTP Servers and scanner components.	Refer to MailMarshal SMTP documentation.
□	**3.** Configure firewalls	"Configuring Firewall Settings" on page 32.
□	**4.** Install the Administrator Server and web console.	"Installing the MailMarshal SPE Administrator Web Console" on page 40.
□	**5.** Run the Database Wizard to create or set up a MailMarshal SPE database connection.	"Running The Database Wizard" on page 47.
□	**6.** Install the Customer Console.	"Installing the MailMarshal SPE Customer Web Console" on page 43.
□	**7.** Create connections to Array Managers and MailMarshal SMTP Servers to connect them with MailMarshal SPE.	"Creating Array Entries" on page 57 and "Configuring MailMarshal SMTP Entries" on page 59
□	**8.** *If you want to customize branding of the Customer Console*, configure the top banner look by supplying your own Service Provider logos and text.	"Configuring Service Provider Branding" on page 50.

☑	Steps	See Section
□	**9.** Run Web Console’s Global Configuration as necessary to configure product settings and Administrator notifications.	“Managing Global Configuration” on page 52.
□	**10.** Configure MailMarshal SPE to use existing Logging Server(s).	“Configuring The MailMarshal SMTP Database” on page 59.
□	**11.** For each customer site, install Connector Agent using the standalone installer.	“Understanding the Connector Agent” in the *User Guide*

INSTALLING PREREQUISITE SOFTWARE

Before installing MailMarshal SPE, install any prerequisite software the MailMarshal SPE components require. Pre-installing the prerequisites will help to isolate any installation issues and also will avoid the requirement to restart your computer during the product installation process.

In addition to the named prerequisites, you must install Microsoft SQL Server on the database server(s) you plan to use.

For more information about required software for each computer in your MailMarshal SPE configuration, see “Hardware and Software Requirements” on page 22.

INSTALLING THE MAILMARSHAL SPE ADMINISTRATOR WEB CONSOLE

Setup installs the MailMarshal SPE Administration Web Console as a new website (and application pool) under IIS, using the default port 80. Setup will stop the Default website.

Note: *You can modify the port, and add HTTPS support, after you complete installation. If you install the Administration and Customer web consoles on the same server at the same time, installation allows you to enter a Host Header value for each site. You must configure name resolution to allow both sites to be used. In this case the installer offers to make entries in the local server Hosts file so that you can quickly access both consoles.*

To install MailMarshal SPE Administration Web Console:

1. Ensure you have installed all prerequisite software specified for the installation. For more information, see “Web Console Installation Requirements” on page 23 and “Installing Prerequisite Software” on page 39.

2. Log on to the computer you plan to use as the server for this Web Console. Use an account that is a member of the local Administrators group.

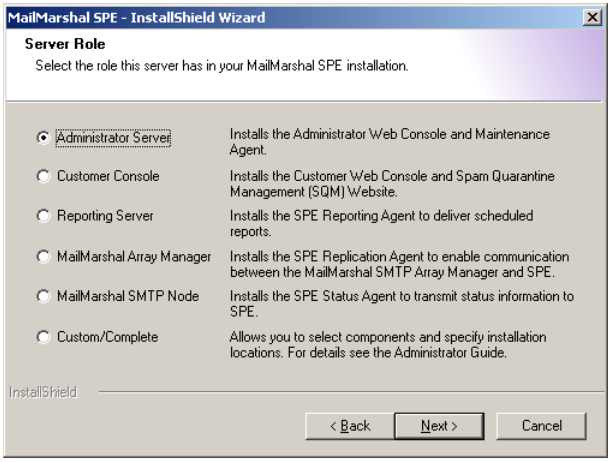
3. Close any open applications.

4. Run the MailMarshal SPE installer.

5. On the Welcome window, click **Next.**

6. On the License Agreement window, carefully read the license information. Select *I accept the terms of the license agreement,* and then click **Next.**

7. On the Server Role window, select **Administrator Server**. Click **Next.**



MailMarshal SPE - InstallShield Wizard

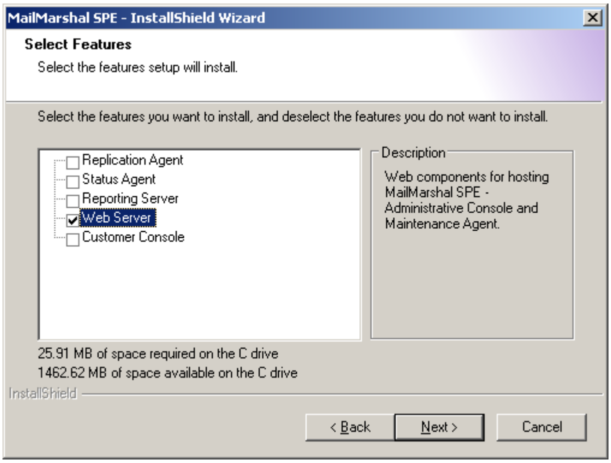
Server Role

Select the role this server has in your MailMarshal SPE installation.

● Administrator Server	Installs the Administrator Web Console and Maintenance Agent.
○ Customer Console	Installs the Customer Web Console and Spam Quarantine Management (SQM) Website.
○ Reporting Server	Installs the SPE Reporting Agent to deliver scheduled reports.
○ MailMarshal Array Manager	Installs the SPE Replication Agent to enable communication between the MailMarshal SMTP Array Manager and SPE.
○ MailMarshal SMTP Node	Installs the SPE Status Agent to transmit status information to SPE.
○ Custom/Complete	Allows you to select components and specify installation locations. For details see the Administrator Guide.

Note: *You can install additional components on the same server, if required, using the Custom/Complete installation type. In particular, the Reporting Agent is commonly installed with the Web Console.*

8. ***If you want to choose the installation location,*** on the Server Role window select **Custom/Complete,** and on the Select Features window select **Web Server.**



MailMarshal SPE - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- □ Replication Agent
- □ Status Agent
- □ Reporting Server
- ☑ Web Server
- □ Customer Console

Description

Web components for hosting MailMarshal SPE - Administrative Console and Maintenance Agent.

25.91 MB of space required on the C drive
1462.62 MB of space available on the C drive

Then click **Next** to continue to the Choose Destination Location window and change or customize location as required.

9. Continue to the Ready to Install window, and click **Install.** The setup program displays a progress bar until all selected components are is installed.

10. On the Database Settings window, create or edit a MailMarshal SPE database connection. For more information, click **Help.** To use an existing database, see “Running The Database Wizard” on page 47

    a. In the SQL Server Name field, specify the name of the Microsoft SQL Server.

    b. Enter a database name

c. Specify a User Name and Password that has permissions to create and populate tables in the database.

d. If required, select the checkbox *Connect using TCP/IP Protocol.* This option is applicable where the database server is behind a firewall. TCP port 1433 must be opened through the firewall in this case.

11. Click **Next.** Database Wizard displays a progress bar until the database connection is complete.

12. On the Finished window, ensure *Start MailMarshal SPE Maintenance Agent* is selected, and then click **Finish.**

INSTALLING THE MAILMARSHAL SPE CUSTOMER WEB CONSOLE

Setup installs the MailMarshal SPE Customer Web Console as a new website (and application pool) under IIS, using the default port 80. Setup will stop the Default website.

Note: *You can modify the port, and add HTTPS support, after you complete installation. If you install the Administration and Customer web consoles on the same server at the same time, installation allows you to enter a Host Header value for each site. You must configure name resolution to allow both sites to be used. In this case the installer offers to make entries in the local server Hosts file so that you can quickly access both consoles.*

To install MailMarshal SPE Customer Web Console:

1. Ensure you have installed all prerequisite software specified for the installation. For more information, see “Web Console Installation Requirements” on page 23 and “Installing Prerequisite Software” on page 39.
2. Log on to the computer you plan to use as the server for this Web Console. Use an account that is a member of the local Administrators group.
3. Close any open applications.
4. Run the MailMarshal SPE installer.
5. On the Welcome window, click **Next.**
6. On the License Agreement window, carefully read the license information. Select *I accept the terms of the license agreement,* and then click **Next.**
7. On the Server Role window, select **Customer Console**. Click **Next.**

Note: *You can install additional components on the same server, if required, using the Custom installation type.*

8. ***If you want to choose the installation location,*** on the Server Role window select **Custom,** and on the Select Features window select **Customer Console.** Then click **Next** to continue to the Choose Destination Location window and change or customize location as required.
9. Continue to the Ready to Install window, and click **Install.** The setup program displays a progress bar until all selected components are is installed.

10. On the Database Settings window, create a MailMarshal SPE database connection. If you have already created a database as part of the Administration Console installation, you should select that database. For more information about the fields, click **Help.**

    a. In the SQL Server Name field, specify the name of the Microsoft SQL Server.

    b. Enter the database name.

    c. Specify a User Name and Password that has permissions to create and populate tables in the database.

    d. If required, select the checkbox *Connect using TCP/IP Protocol.* This option is applicable where the database server is behind a firewall. TCP port 1433 must be opened through the firewall in this case.

11. To connect (and create the database if it does not exist), click **Next**.

12. On the Finished window, click **Finish.**

INSTALLING MAILMARSHAL SPE AGENT SERVICES

The Agent Services are processes that allow MailMarshal SPE to communicate with MailMarshal SMTP Array Managers, MailMarshal SMTP Servers, and MailMarshal SPE Reporting Servers. The Agent Services are installed on each server:

- **Replication Agent** for every MailMarshal SMTP Array Manager installation.
- **Status Agent** for every MailMarshal SMTP Server installation.
- **Reporting Agent** on a standalone server, the MailMarshal SPE Web Console server, or the MailMarshal SPE database server.

The installer allows you to install one or more of the services depending on the server roles of each computer.

If you later want to specify new arrays and servers, you can re-run the installer on the target computer as needed.

Each MailMarshal SPE Agent requires you to set up a database connection in order to function correctly.

Each MailMarshal SPE Agent requires outbound SMTP access to the notification SMTP server as specified in the Web Console under Global Configuration or array settings.

For more information about MailMarshal SPE environments, see “MailMarshal SPE Architecture” on page 16 and “Hardware and Software Requirements” on page 22.

To install Agent Services:

1. Ensure you have installed all prerequisite software specified for the installation. For instance, to install the Replication Agent you must first install the Array Manager component from MailMarshal SMTP Setup. For more information, see “Agent Services Installation Requirements” on page 25 and “Installing Prerequisite Software” on page 39.
2. Log on to the computer where installation is required, using an account with local Administrator privilege.
3. Close any open applications.
4. Run the MailMarshal SPE installation program.
5. On the Welcome window, click **Next.**
6. On the License Agreement window, carefully read the license information. Click **I accept the terms of the license agreement,** and then click **Next.**

7. On the Setup Type window, select the appropriate server role, and then click **Next.**

Note: *To install more than one Agent Service, or to customize the installation location, select Custom installation and choose services from the list.*

8. On the Ready to Install window, click **Install.** The setup program displays a progress bar until the program is installed.
9. Setup prompts you to create or edit MailMarshal SPE database connection settings using Database Wizard. You can complete this task now or click **Cancel** to perform it later. For more information, see “Running The Database Wizard” on page 47.

Note: *If database connection information is not available in the Registry when an Agent starts up, the Agent checks the Registry every five minutes until valid information is available.*

10. The Database Wizard displays a summary showing the services connected.
11. On the **Finished** window, select the Agents to be started, and then click Finish.

RUNNING THE DATABASE WIZARD

As part of the installation process for Web Console or any Agent Services, you must run the Database Wizard to configure MailMarshal SPE Agents to function correctly.

By default installation runs the Database Wizard when you install a component that requires this connection. If you choose to skip this step or you do not have the database connection information available at the time of installation, you can start Database Wizard from the Windows Start Menu on each server at a later time.

You can also re-run Database Wizard if the connection information changes.

The purpose of running the Database Wizard is to identify the MailMarshal SPE database source. MailMarshal SPE Web Consoles and Agent Services require a connection to the database for data storage and retrieval.

Ensure you have started the Microsoft SQL Server and that the database server is accessible from the computer running Database Wizard.

To run the Database Wizard:

1. Ensure that all MailMarshal SPE agent services and web console sites are stopped.
2. If the Database Wizard is not running, run the program from the start menu shortcut.
3. On the Database Settings window, enter the database connection details to connect to the database server. For more information, click **Help.**
    a. In the SQL Server Name field, specify the name of the Microsoft SQL Server.
    b. Specify a User Name and Password that has permissions to create and populate tables in the database.
    c. If required, select the checkbox *Connect using TCP/IP Protocol.* This option is applicable where the database server is behind a firewall. TCP port 1433 must be opened through the firewall in this case.
4. ***If you want to create a new database,*** in the Database Name field enter a new database name (not present on the server).

Note: *All components in an installation must connect to the same database.*

5. ***If you want to use an existing MailMarshal SPE database:***

    a. In the Database Name field, enter the name of an existing MailMarshal SPE database. Database Wizard will check for a valid MailMarshal SPE database. If the database is not valid, you will be prompted for further options.

    b. Ensure the checkbox **Recreate the database** is **not** selected.

    c. Click **OK.** Database Wizard displays a progress bar until the database connection is set up.

6. ***If you want to overwrite an existing database:***

    a. In the Database Name field, enter the name of an existing database.

    b. Select the checkbox **Recreate the database to** overwrite the specified database even if it is not empty.

    Note: *Perform a backup before overwriting any existing databases.*

7. On the MailMarshal SPE Database Setup window, review the Database field, then click **Close**.

For more information about the MailMarshal SPE database, see “Managing Global Configuration” on page 52, “Creating Array Entries” on page 57, “Configuring MailMarshal SMTP Entries” on page 59, and “Configuring The MailMarshal SMTP Database” on page 59.

CONFIGURING SERVICE PROVIDER BRANDING

The Customer Web Console and SQM site can be branded for the service provider and in some cases for individual customers. Available functionality includes:

- Product name and company name setting.
- Customized logo for each reseller and/or customer.
- Customized application theme for the Customer Console.
- Documentation link for the Customer Console.
- Customized and user selectable application theme and language pack for the SQM pages.

***Tip:** If you use more than one Customer Console web server, the themes and documentation link can be set for each server.*

Product Name and Company Name

You can set values for the product name and your company name on the Global tab of System Settings. See “System Settings” on page 53. These values are used in email messages such as password delivery and reset messages, and SQM new account messages.

Customized Logos

The console product logo image can be changed for individual resellers and/or customers. See “Configuring Resellers, Customers and Domains” on page 71.

***Note:** This setting does not affect the logo used on the login page. You can change this logo within the application theme.*

Application Theme for the Customer Console

You can create a custom Application Theme.

1. Make a copy of the subfolder `App_Themes/Default` (found in the Customer Console folder of the MailMarshal SPE installation).
2. Edit your copy. Make any changes required to styles and graphics.
3. To use the new theme, edit the file `web.config` (found in the Customer Console folder of the MailMarshal SPE installation). Locate the following line:

   ```
   <pages theme="Default" >
   ```

   Change the name to reference your new theme.

Notes: *When editing style and CSS files be aware that these files include explicit references to images in the Default theme folder. If you are making major changes, you may wish to globally replace these references. If you are only making minor changes, you may want to leave the references to the default images.*

When the product is upgraded, the Default theme will be overwritten but custom themes will not be changed.

Documentation Link for the Customer Console

To customize the documentation page (linked from the header of the Customer Console), edit the HTML File `branding\documentation.html`

If this file is not present, the Documentation link will not display.

Application Theme and Language Pack for SQM pages

You can create multiple themes and language packs for the SQM pages, in addition to the items provided by default. For more information, see M86 Security Knowledge Base article Q12237.

MANAGING GLOBAL CONFIGURATION

After you install MailMarshal SPE Web Console, run the Database Wizard, and create customized branding, you can log on to the Administration Web Console to complete initial configuration of the MailMarshal SPE system.

Initial configuration includes:

- Organizing System Settings
- Editing security settings, including IP Access to the Web Console, Administrator logins, and Customer groups you can use to limit administrative powers.

For more information, see “Understanding the Administration Web Console” on page 63.

To log on to Administration Console and manage global configuration:

1. Log in to the MailMarshal SPE Web Console server.

Note: *To access the Administration Web Console for the first time, you must be logged on to the server computer. You can allow access from other computers; see “IP Access” on page 55.*

2. Using Internet Explorer, connect to your MailMarshal SPE website (by default, as `http://localhost`). A login page displays.
3. In the Login Name field, type `admin@admin` (default Administrator credential).
4. In the Password field, type `admin` (default Administrator password).
5. Click **Log in** to proceed to the Web Console.
6. In the left pane, expand **Global Configuration.**
7. Continue with System Settings.

8. Once System Settings have been configured, additional items will be available in the left pane. Continue with IP Access or Administrative Logins.

***Important: It is essential to change the default username and/or password for the three Administrator accounts created by the installation**.*

- *By default, the Web Console allows administrative logins only from the local Web Console server. To allow and manage access from other locations, see the IP Access item in the Administration Web Console menu tree.*
- *If the master Administrator account is locked out (due to repeated failed logins) it can always be used by logging in directly from the Web console server (using* `http://localhost`*),*

System Settings

The System Settings configuration includes the following tabs. You should set appropriate values in each field. For details of the fields, click **Help**.

Global

Configure the default website wide settings to be used by MailMarshal SPE. For instance, you may want to forward general email notifications to the designated Site Administrator.

***Note:** Dynamic DNS for incoming mail, previously configured here, has been replaced by the Forward to Host setting in Domain setup.*

Notifications

Set the email addresses used by MailMarshal SPE to notify Administrators about processing problems, trial expiration, system errors and message queue limits.

Security

Configure the passwords, session timeouts, and login lockout periods for the Web Console.

Agent Logging

Configure the retention periods for MailMarshal SPE Agent log files.

SMTP

The SMTP server settings are used by Web Console to deliver notification messages. The server used for notifications should be located outside of the MailMarshal SPE architecture, so that notifications can be successfully sent in event of a server failure.

Proxy

MailMarshal SPE services communicate by HTTP to external addresses such as the M86 licensing website. If you use MailMarshal SPE through a proxy, configure the proxy server details to allow indirect connections to other network services.

SQL

Specify a SQL login used by the Web Console service to link to MailMarshal SMTP and SPE databases. This user must specifically have administrative privileges on all servers.

Registration

Enter the license key for your organization as provided by M86. MailMarshal SPE must connect to the M86 licensing website to complete licensing (`https://activations.marshal.com`).

MANAGING SECURITY CONFIGURATION

The Security Configuration section of the Web Console allows you to control access to the administrative functions of MailMarshal SPE. You can limit access by IP range. You can set up and manage administrative logins. You can set up customer groups that allow you to easily control which customers' settings can be managed by each administrator.

IP Access

IP Access configuration allows you to control access to the MailMarshal SPE Web Console Administration area. By default you can only access the Web console administration area from the local server. You can control access by entering one or more IP address ranges to allow or deny. The permissions for an address are determined by evaluating the entries in top down order as they appear in the list.

To configure IP Access, add or edit one or more address range entries. Then set the order of evaluation by highlighting an entry and clicking **Up** or **Down.**

For more details, see **Help**.

Administrative Logins

Admin Logins configuration allows you to create administrative logins for the MailMarshal SPE installation, and configure the areas of the consoles that each login is allowed to access. For details of the fields, see Help.

Note: *MailMarshal SPE creates three administrative logins by default:*

- ***SPE Administrator:*** *the default* `admin` *login*
- ***SPE Site Admin:*** *allows Service Provider staff to log in as an administrator of any customer, with full permission to change settings. Log in as* `sitelogin@customerdomain.`
- ***SPE Support:*** *allows Service Provider staff to log in as an administrator of any customer, with read access only. Log in as* `supportlogin@customerdomain.`

You can create additional logins with any of these privileges. MailMarshal SPE will not allow you to assign the Site Admin or Support privileges to a login if a login with the same name already exists in a customer domain.

Use the Site Admin login with caution. *The consoles do not prevent simultaneous users making conflicting changes in a customer's configuration. Errors in configuration could result.*

General

Enter the Administrator's details and login password to grant access to the Administrators Console. You can choose to allow read-only access.

Menu Security

For cases that requires more granular permission management, change the Menu Security to allow or disallow the viewing of certain menus.

Customer Provisions

Use the fields on this tab to grant or deny access from the login to specific customers' settings. This tab is not available for the SPE Administrator, because it always has access to all customers.

Customer Groups

You can use Customer Groups to control which customers' settings can be managed (Site Login or Support Login) by individual Administrative Logins. Once you have assigned customers to a group, you can assign management of the group to a new login with no need to re-select each member (using the Customer Provisions tab of the login properties). For details of this functionality, see Help.

CREATING ARRAY ENTRIES

The Array entries allow MailMarshal SPE to communicate with the managed MailMarshal SMTP Arrays through their respective Array Managers. The properties of an Array entry include advanced configuration options that allow you to control reload scheduling, relaying sources, hosts security, IP Security, DoS protection and Internet access options. For more information about editing Array entries and advanced Array Manager configuration see “Configuring Arrays” on page 83.

To create an Array entry:

1. Using a Web browser, log in to the MailMarshal SPE Administration Web Console.
2. In the left pane, expand Server Configuration.
3. Click **Arrays.**
4. On the main window click **New.**

5. On the New Array window, specify the following information:

   a. On the General page, enter the name, description, and time zone of the Array Manager. Click **Next** to proceed.

   b. Specify the IP address and MailMarshal SMTP access port of the Array Manager, and the MX record (in FQDN format) used to deliver email to the array, and then click **Next.** If you do not know the required information, contact the Administrator of the MailMarshal Array Manager.

   c. On the SMTP window identify the SMTP server and domain this array can use to send MailMarshal SPE notification messages, and then click **Next.**

   d. On the Notifications window enter details of the array Administrator, and notification email addresses for the listed array events. Click **Next.**

   e. On the Credentials window, specify a Windows identity that the Web Console can use to connect to the Array Manager

   f. On the Policy Groups window, select the Policy Groups that you want this array to apply to all email it processes. To learn about creating Policy Groups, see “Creating Policies and Policy Groups” on page 165.

6. Review the previous details by clicking **Back** and **Next** to navigate the wizard. Click **Finish** on the final window to save settings and close the window.

⚠ ***IMPORTANT Credentials information:*** *MailMarshal SPE communicates with the remote array manager using these windows credentials. If you are not using a domain, enter the name of the WORKGROUP that the array manager belongs to.*

7. You must edit each server in the array to provide basic information before you can use the array. See “Configuring MailMarshal SMTP Entries” on page 59.

Configuring The MailMarshal SMTP Database

Each Array Manager uses a MailMarshal SMTP Database (also known as a Logging Server) to store email history and configuration. MailMarshal SPE will automatically link the logging server during creation of the array entry.

Note: *To enable MailMarshal SPE to access the MailMarshal SMTP databases, in MailMarshal SMTP you cannot specify the database server location using a loopback address. Do not use the values* `localhost` *or* `127.0.0.1` *even if the MailMarshal SMTP database is located on the same computer as the Array Manager. For instance, you can specify the server as* `192.168.1.1` *or* `MMServer.`

To change the MailMarshal SMTP Database settings for an Array:

1. On the main window, select the array, and click **Edit.**
2. Select the Database tab.
3. ***If your Logging Server resides on the same machine as the MailMarshal SPE Database,*** select the **Local Server** checkbox.
4. Enter the server address and alias of the server instance if necessary.
5. Specify the database and the corresponding Username and Password.

CONFIGURING MAILMARSHAL SMTP ENTRIES

When you add Array Manager entries to MailMarshal SPE, the email processing servers in each array are also added. You must edit the entry for each server to provide basic information about it.

You can edit information about each server, and enable, disable, or delete it at any time.

Notes: *Deleting a server does not remove it from the MailMarshal SMTP array. Deleting only un-links the server within MailMarshal SPE.*

- *To add or delete email processing servers in an array, use the MailMarshal SMTP Configurator for that array.*
- *If you add, delete, or change an email processing server in a MailMarshal SMTP array, you must update the array information in MailMarshal SPE. To automatically update the array information, in MailMarshal SPE, edit the array and save it (by clicking **OK**). This action will automatically update the list of servers available for that array.*

To edit a MailMarshal Server entry:

1. In the left pane, expand Server Configuration.
2. Click **MM Servers**.

Note: *This menu is only available after at least one Array Manager has been added in the Web Console.*

3. Select a server, and then click **Edit.**
4. On the MailMarshal Server window, edit the connection details for the MailMarshal SMTP server. See **Help** for details.
5. If you need to override the proxy setting for Web access from this server (used by SpamProfiler updates), click the Internet Access tab and enter the required information. See **Help** for details.
6. Click **OK** to save the settings and close the window.

You can also disable or enable (temporarily stop or resume) the operation of a SMTP Server.

To disable/enable a SMTP Server entry

1. In the left pane, expand Server Configuration.
2. Click Servers and select a Server entry on the main pane.
3. Click **Enable** or **Disable** to control whether the MailMarshal SPE installation will include the selected Server.

Warning: *Disabling a server does not stop email flow.*

Upgrading MailMarshal SPE

This release of MailMarshal SPE supports upgrade from version 2.2 and above. For more information, see the Release Notes. The document *Migrating MailMarshal SPE to Version 3.0* provides information about how to move components in order to take advantage of the new website architecture in version 3.0

You can upgrade MailMarshal SPE to the latest version by running the setup program for the new version on each computer on which you installed MailMarshal SPE Web Console or Agent Services. To learn about specific upgrade issues and prerequisite changes for a version, see the Release Notes

IMPORTANT: *You MUST update all components to the same version.*

- *Before upgrading, stop ALL MailMarshal SPE components and agents on all servers. Affected servers will include at least the MailMarshal SMTP Array Managers and processing servers, and the MailMarshal SPE Web Console servers. The Database Wizard attempts to check for services that may be running throughout the MailMarshal SPE installation, and warns you to stop services. If you have verified that all agents and services are stopped, you can continue past the warning.*

To add or remove installed components of MailMarshal SPE on a server, you must run the installer from its original location. You *cannot* use the Modify function of Add/Remove Programs from the Windows Control Panel.

UNINSTALLING MAILMARSHAL SPE

The following steps provide general guidelines for the steps required to remove MailMarshal SPE from your systems. When you uninstall MailMarshal SPE, you will no longer be able to use any of the Agent Services to update or view MailMarshal SMTP Array Manager/Server settings.

To uninstall MailMarshal SPE:

1. .***On each computer where MailMarshal SPE Agent Services were installed,*** use Add/Remove Programs from the Windows Control Panel to remove MailMarshal Agent Services.
2. On the web server computer(s), use Add/Remove Programs from the Windows Control Panel to remove the Administration and/or Customer Web Consoles.
3. ***If you want to remove the MailMarshal SPE database from Microsoft SQL Server,*** complete this task using SQL administration tools such as Enterprise Manager.
4. ***If you want to remove MailMarshal SMTP products completely,*** follow the uninstall steps in the *MailMarshal SMTP User Guide*.

Chapter 4
Understanding MailMarshal SPE Administration

MailMarshal SPE provides a website interface for service providers, and a separate website for customer administration and end-user quarantine management of the system.

This chapter presents material on the Administration Web Console only. Please see the *User Guide* for details on customer-side features. Administrators should be familiar with the Customer Console, which they can log in to for troubleshooting purposes.

UNDERSTANDING THE ADMINISTRATION WEB CONSOLE

To access the MailMarshal SPE Administrator Web Console, use Microsoft Internet Explorer 6 or above. You must allow JavaScript and cookies from the Web Console. The Web Console does not use any Flash or ActiveX components, and can safely be added into the “Trusted Sites” Zone within your browser.

Note: *You can connect using other browsers, and you may be able to access many functions, but only Internet Explorer is supported. Significant parts of the interface use IE specific functionality.*

To start the Administrator Web Console, start Internet Explorer, and enter the address of your MailMarshal SPE website.

Important: *The Web Console does not restrict multiple users from editing configuration and policy at the same time. Conflicting changes could be made, and in some cases email flow or customer configuration could be affected. To avoid potential problems,* ***only one user authorized to make changes should be logged in to the Administration Web console at a time.***

Only one user authorized to make changes should be logged in to each customer domain at a time.

This issue does not affect the Dashboard, Mail History, Message Queues management, Audit History, Reports, or "read only" access to any part of the Console. Multiple users can access these items at the same time without concern.

Logging into the MailMarshal SPE Administration Console

When you start the Web Console, you will be asked for user authentication to continue MailMarshal SPE log on. Access to the various sections of the site is limited by the permissions associated with each login credential.

Note: *The password is case sensitive.*

Use the default master account for your first log on as Administrator:

User Name: `admin@admin`

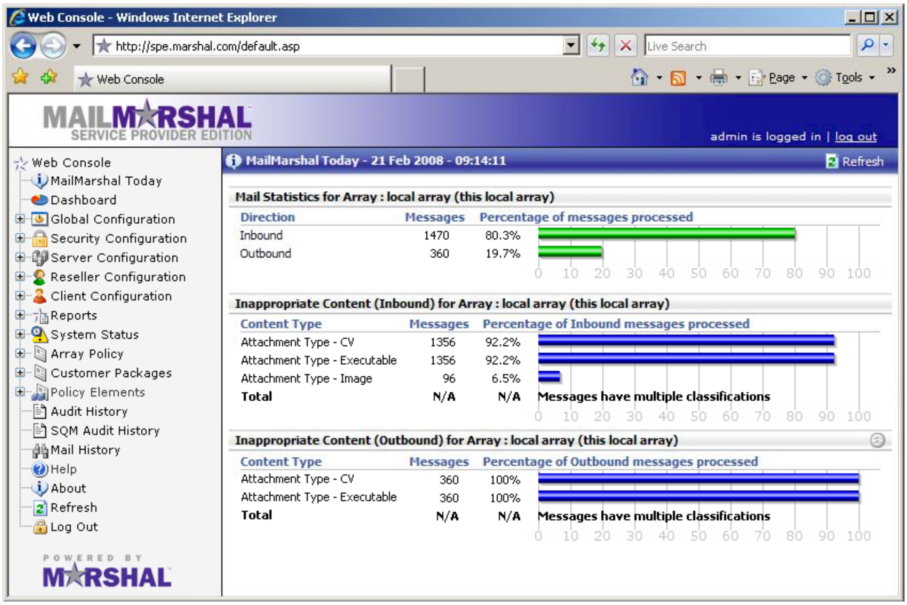
Password: `admin`

IMPORTANT NOTE: *Change the password of the default Administrator account immediately.*

You can leave the Administration Web Console by simply closing your browser window. Alternatively you can click the logout link on the top pane (see next section). By default, Administration Web Console has an inactivity timeout of 20 minutes. This feature is designed to protect the Web Console when you leave the work station unlocked for an extended time.

Understanding The MailMarshal Today Page

The MailMarshal Today page displays a quick overview of daily statistics of the MailMarshal SPE infrastructure.



MailMarshal Today - 21 Feb 2008 - 09:14:11

Mail Statistics for Array : local array (this local array)

Direction	Messages	Percentage of messages processed
Inbound	1470	80.3%
Outbound	360	19.7%

Inappropriate Content (Inbound) for Array : local array (this local array)

Content Type	Messages	Percentage of Inbound messages processed	
Attachment Type - CV	1356	92.2%	
Attachment Type - Executable	1356	92.2%	
Attachment Type - Image	96	6.5%	
Total	**N/A**	**N/A**	**Messages have multiple classifications**

Inappropriate Content (Outbound) for Array : local array (this local array)

Content Type	Messages	Percentage of Outbound messages processed	
Attachment Type - CV	360	100%	
Attachment Type - Executable	360	100%	
Total	**N/A**	**N/A**	**Messages have multiple classifications**

Information available on this page includes the following items for each array:

Mail Statistics

Shows the number of messages and volume of traffic for the current day, divided into inbound and outbound traffic. Inbound traffic is email addressed to the local domains as configured in MailMarshal SPE.

Inappropriate Content

Shows the number of messages that MailMarshal has classified as inappropriate (usually including spam and virus infected messages). The data can include one or more message classifications that you configure.

Understanding the Dashboard

The Dashboard displays a quick overview of server health, and more detailed statistics on email traffic, blocked messages, and other MailMarshal actions. To view the Dashboard, in the left pane expand **Server Status** and then click **Dashboard**. For details of the available options, see Help.

Working With the Content Menu

The MailMarshal SPE Administration Web Console displays three panes:

- The top pane allows Service Provider branding, which you can customize as discussed in “Configuring Service Provider Branding” on page 50.
- The left pane is the menu pane for all administrative configuration.
- The right pane 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.

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 by clicking the menu item. View detailed properties of an item by clicking it then use the right pane for detailed information.

Working With the Details and Results Pane

The details and results pane in MailMarshal SPE is context dependent.

- In most cases a Help link displays at the top right. Help provides detailed information about the page purpose and the fields.
- Many fields include an Info tooltip that provides basic information about the field.
- On data entry forms, a field with a blue background indicates that you must enter or change data before submitting the form.

- The pane often shows a list of items and a number of action buttons.
  - You can usually sort the list by clicking column headers.
  - You can make changes to an item by selecting it and clicking the appropriate button.
  - You can right-click an item to see a list of available actions.
  - In many cases you can also double-click an item to perform a default action.

Please refer to the individual chapters and Help for descriptions of the fields on each view.

- For the Array and MailMarshal Server menu, see “Configuring Arrays” on page 83 and “Configuring MailMarshal SMTP Entries” on page 59.
- For the Client and Domain menu, see “Configuring Customers” on page 75 and “Setting Up Email Domains” on page 79.
- For the Email Policies menu, see Chapter 6, “Understanding Email Policy Elements.”
- For the Reports, Messages, Audit Menu, see Chapter 9, “MailMarshal SPE Monitoring, Auditing, and Reporting.”

Working with RSS Feeds

MailMarshal SPE provides RSS news feeds from M86 in the Administration Web Console. These feeds allow you to learn about important product updates and security alerts from M86.

To view the news feed information, in the left pane of the Console expand the item **News Feeds,** and then select a feed. The article titles display in the right pane. To view an article, click the title. If you do not see the news Feeds item, check the MailMarshal SPE proxy settings.

You can search the feed information, and subscribe to the feed so that you can read it in another news reader of your choice. See the controls and links in the right pane of the console.

You can provide a RSS feed to customers that will display in the Customer Web Console. To create a feed, place a file named `rss.xml` in the folder `RSS` within the MailMarshal SPE Website folder. You can create the feed using one of the many RSS feed creator packages available.

Data Entry in MailMarshal SPE

The details and results pane includes various forms for user input:

- Popup wizards for adding new items.
- Popup property pages for editing existing items.
- Property tabs for global configuration.
- Search fields for query (report, message tracking, auditing) purposes.

All of the above forms use a standardized MailMarshal SPE interface. Various controls have been provided to automatically validate user input. These include:

- Email Address
- Fully Qualified Domain Name
- IP Address
- Phone Number

Fields marked with a blue background indicate that the field requires data. Either a required field is empty, or the current data in the field is invalid)

Tip: *Hover the cursor above the [icon I] icon to see a short descriptive hint about a field.*

UNDERSTANDING AGENT SERVICES

MailMarshal SPE includes four Agent services:

Maintenance Agent

Provides performance optimization and manages temporary data retention for the Web Console server and the database. This agent must always be running and is installed on the same server as the web console.

Replication Agent

A Replication Agent is installed on every MailMarshal Array Manager that is managed by MailMarshal SPE. The Agent provides integration between MailMarshal SPE and the Array Managers, including policy updates.

Reporting Agent

Performs regular data mining and reporting functions from the SPE SQL Server.

Status Agent

A Status Agent is installed on each MailMarshal SMTP Server that is managed by MailMarshal SPE. The Agent supplies real-time notifications about the servers’ conditions to MailMarshal SPE.

All of the Agent Services are background processes that are started when Windows starts.

To start or stop the process manually, use the Windows Service control manager.

The refresh rate of the Agent Services is defined as follows:

Agent Service	Refresh Every	Notes
Maintenance Agent	5 minutes	

Agent Service	Refresh Every	Notes
Replication Agent	• *Depends on the Schedules set in the Array Properties* • *The minimum refresh time is every 15 minutes*	• *A **Reload** button is available in Web Console to force Replication Agent to make changes to Array Managers.* • *Actions taken by Replication Agent may take up to 90 seconds to perform. This is due to technical reasons in restarting Windows and MailMarshal services*
Reporting Agent	60 minutes	
Status Agent	1 minute	

Additional information about Agent Services is available in the log files and Event Logs. For more information, please see “Monitoring Agent Services” on page 228.

UNDERSTANDING OTHER TOOLS

The Database Wizard tool allows you to change settings related to communication with the MailMarshal SPE SQL Database Server. The Database Wizard tool can also be used to upgrade and to recreate the database in case of corruption. These settings cannot be changed from within other interfaces for technical reasons.

The Connector Agent allows LDAP and/or Active Directory user groups to be synchronized from a customer’s environment to the MailMarshal SPE envorinment, using HTTP and HTTPS to connect to the Customer Web Console server.

Chapter 5
Managing MailMarshal SPE

This chapter discusses a number of configuration options and tasks that maintain and customize your MailMarshal SPE environment.

Configuring Resellers, Customers and Domains

MailMarshal SPE provides a powerful and flexible framework that allows you to manage email content security policy for organizations of many sizes, from small and medium customers with one domain to enterprise customers with several hundred domains.

You can enter details of resellers. You can associate customers with resellers for reporting and branding purposes.

Configuring Resellers

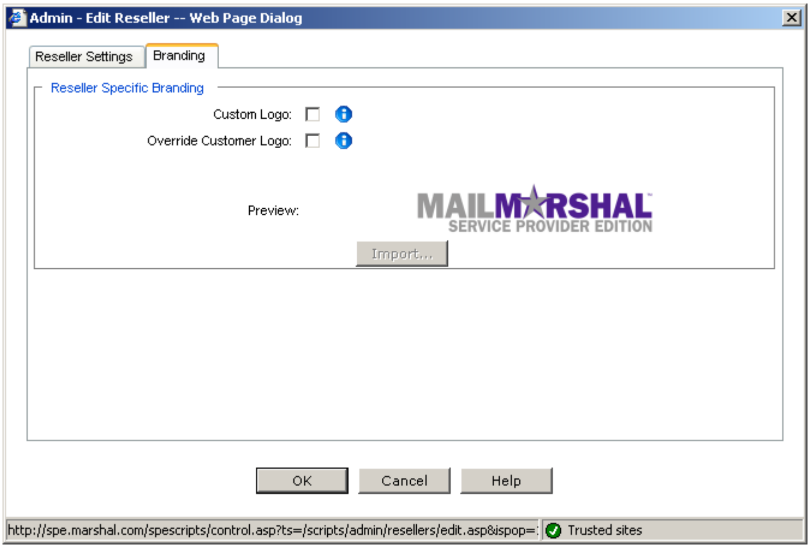
A Reseller entry consists of contact information and optional site branding with a custom logo. You can assign customers to resellers. You can create Reseller Site and Support logins to allow a Reseller to view and manage site settings for their customers.You can report on customer and licence activity by reseller with the Reseller Detail and Reseller Summary reports.

To review and configure Resellers:

1. In the left pane of the Administration Console, expand the item Reseller Configuration.
2. Select the item **Resellers.**

3. ***If you want to create a new Reseller entry,*** click **New.** Enter the identifying information for the Reseller, then click **OK.**

Note: *To configure the site logo displayed for customers of a reseller, edit the entry after creating it, and view the* ***Branding*** *tab. For details of this tab, see* ***Help****.*


Admin - Edit Reseller -- Web Page Dialog
Reseller Settings
Branding
Reseller Specific Branding
Preview:
MAILMARSHAL
SERVICE PROVIDER EDITION
Import...
OK
Cancel
Help
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/admin/resellers/edit.asp&ispop=
Trusted sites

Custom Logo: □

Override Customer Logo: □

4. ***If you want to edit a Reseller entry,*** select it and then click **Edit.** Review and change the information on each tab, and then click **OK.** See **Help** for details of the fields on each tab.

To manage Reseller logins:

1. In the left pane of the Administration Console, expand the item Reseller Configuration.

2. Select the item **Reseller Logins.**

Note: *This item is only present when at least one Reseller has been configured.*

3. To view enabled, disabled, or deleted logins, use the tabs above the listing.

4. To add a login, click **New.**

5. To edit the properties of an existing login, select it and then click **Edit.**

6. For full details of the available actions and properties, see **Help** for each window.

Note: *Reseller logins can only manage customers associated with the specific reseller. If you delete a Reseller entry, all associated reseller logins are also deleted.*

Sample Customer Scenario

The rest of the Administration Guide uses "XYZ Corp" as a sample Customer to illustrate MailMarshal SPE functionality. The organization, domain names and users illustrated are fictitious. Any resemblance to any real XYZ Corporation is purely coincidental.

XYZ Corp uses the following domain addresses throughout the world for email communication.

Domain	Number of Email Addresses	User Base
xyz.com	<60	Email Address for Production staff and Managers
support.xyz.com	<20	Email Address for Support staff
xyzaustralia.com	<10	Email Address for Sales and Consultants in Australia
xyzeurope.com	<10	Email Address for Sales and Consultants in Europe

Managing Customer Licenses

MailMarshal SPE can enforce licensing based on unique email addresses belonging to a customer. For example, in the above scenario XYZ Corp requires 100 licenses (that is, 60+20+10+10).

Note: *Each email alias counts as a separate email address. For example, if both* `joe@xyz.com` *and* `joe@support.xyz.com` *are delivered to the same Exchange mailbox, MailMarshal SPE still counts two licenses. Before linking new domains to an existing customer, ensure that the customer has sufficient licenses.*

You can choose to enforce the license count for a customer. You can pass through, or block, email that is unlicensed.

- If you choose to pass through unlicensed email, outbound messages from unlicensed senders are passed through with no policy applied. Inbound messages have policy applied only for licensed users. A message with several recipients is split if necessary and policy is applied only for the licensed users.
- If you choose to block unlicensed email, if **the sender or any recipient** of a message is licensed, then MailMarshal SPE considers the email to be licensed.

To enforce the license count:

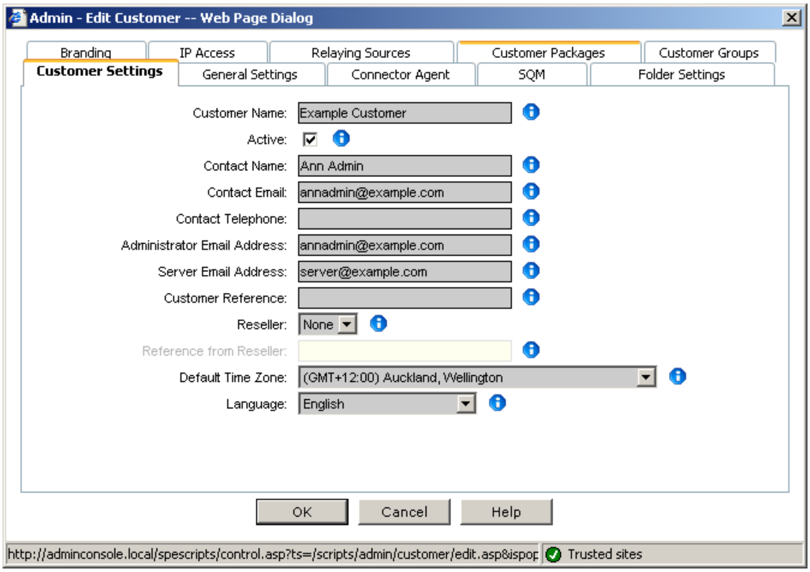
1. When you configure the customer information, select one of the two Enforce License Count options (found on the General Settings tab of the Add or Edit windows). See “Configuring Customers” on page 75.
2. When you configure the arrays that process email for this customer, customize the messages that MailMarshal SPE will apply to unlicensed email (on the Advanced properties window for each array). See “Advanced Options for Array Properties” on page 92.

3. Instruct the customer to enter or import a list of valid email addresses in the Licensed Users user group. For more information, see the *User Guide.*

Note: *Entries in this group must be individual email addresses (not wildcards). The group can also include other users groups, as long as they do not have any wildcard entries. If the customer is using Connector Agent to import addresses, it may be easiest for them to use an imported group.*

Configuring Customers

MailMarshal SPE can provide a range of email content security services to customers. The service scenarios range from minimal anti-virus scanning only, to customer-defined Acceptable Use Policy enforcement at the Service Provider gateway.



Customer Name: Example Customer

Active: ☑

Contact Name: Ann Admin

Contact Email: annadmin@example.com

Contact Telephone:

Administrator Email Address: annadmin@example.com

Server Email Address: server@example.com

Customer Reference:

Reseller: None

Reference from Reseller:

Default Time Zone: (GMT+12:00) Auckland, Wellington

Language: English

http://adminconsole.local/spescripts/control.asp?ts=/scripts/admin/customer/edit.asp&ispop

A Customer entry requires the following information:

- Contact information.
- Customer Administrator Details and Login Account for the MailMarshal SPE Web Console.
- General and Archival Settings for email messages.
- MailMarshal SMTP Array allocation.
- Total number of licensed users for this Customer.

You can also configure a number of other items such as user group retrieval (Connector Agent), additional logins, additional allowed relaying sources, availability of Digests, and branding information.

For each domain linked to the Customer, the following are required:

- Domain name and administrative contact.
- SMTP Delivery information for outbound mails.
- Message Queue Settings.
- Billing information and usage settings.

To review and configure Customers:

1. In the left pane of the Administration Console, expand the item Client Configuration.
2. Select the item **Customers.**
3. ***If you want to view or edit the customer's user logins,*** select **Logins.** You can create, delete, and manage permissions for all customer logins. Permissions control console access and menu views, and access to view and process messages. You can set message permissions for each quarantine folder (Mail Security), for the message sender or recipient (Group Security), and for Deadletters (General tab). For details of the available options, see Help.

4. ***If you want to see the customer's audit history,*** select **Audit.**

5. ***If you want to view the customer's email processing rules,*** select **Rules.**

To create or edit a Customer entry:

1. ***If you want to create a new customer entry,*** on the main window click **New.** Specify the following information:

   a. On the Customer Settings pane, enter the company name, the contact person details, default administrator and server addressees, and your internal reference. Optionally select a Reseller associated with the Customer, and enter a Reseller reference.

   b. On the Administrator Account pane, enter Customer Administrator contact information and the default user login details for the Customer. Choose whether to allow or deny Console access by default.

   c. On the General Settings pane identify locale information for the Customer, allocate an array of MailMarshal SMTP Servers, and set the customer type, number of licenses, license enforcement, and permissions.

   d. On the Connector Agent Settings pane, choose whether this customer can use Connector Agent, and enter the Connector Agent settings.

   e. On the Trial pane, choose whether this is a trial customer and set the expiry date.

   Note: *When a customer trial expires, email for their domains is passed through without any rule action. You can configure a message stamp that will be applied to incoming messages after the trial period expires. See “Advanced Options for Array Properties” on page 92.*

   f. On the Archive Settings pane enter the default retention period for email messages and the number of days to archive messages.

g. On the Customer Packages pane, select the policy packages the customer can use. To learn about creating Packages, see “Understanding Policies and Policy Groups” on page 163.

h. Review the previous details by clicking Back/Next to navigate the wizard. Click **Finish** on the final window to save and close the popup.

Note: *To configure additional settings such as a custom site logo, IP access settings, digesting, delete on release, and relaying settings, edit the customer entry.*

2. ***If you want to edit an existing customer entry,*** on the main window click **Edit.** Click on the respective tabs to review the configured details. The following additional tabs are available:

   - Branding: Configure a custom logo for the customer.
   - Customer Groups: Select the Groups that this customer is a member of. Groups allow you to control the Administrative Logins that can access this customer's settings.
   - IP Access: Configure permission to use the Customer Web console by IP address ranges.
   - Relaying Sources: Configure IP addresses or hosts allowed to relay outbound email from this customer (in addition to the customer’s local domain email servers).

   See **Help** for details of the fields. Click **OK** to save and close the window.

3. ***If you want to deactivate a customer,*** on the main window click **Edit.** On the Customer Settings tab, clear the **Active** checkbox.

Note: *When a customer is deactivated, email for their domains is passed through without any rule action. You can configure a message stamp that will be applied to incoming messages of deactivated customers. See “Advanced Options for Array Properties” on page 92.*

Setting Up Email Domains

A single customer can use multiple email domains. Under the sample scenario for XYZ Corp, four email domains need to be separately managed. The reasons for separate management of domains can include:

- Physical isolation of mail servers
- Presenting different work units under the organization.
- Partitioning of Acceptable Use Policies

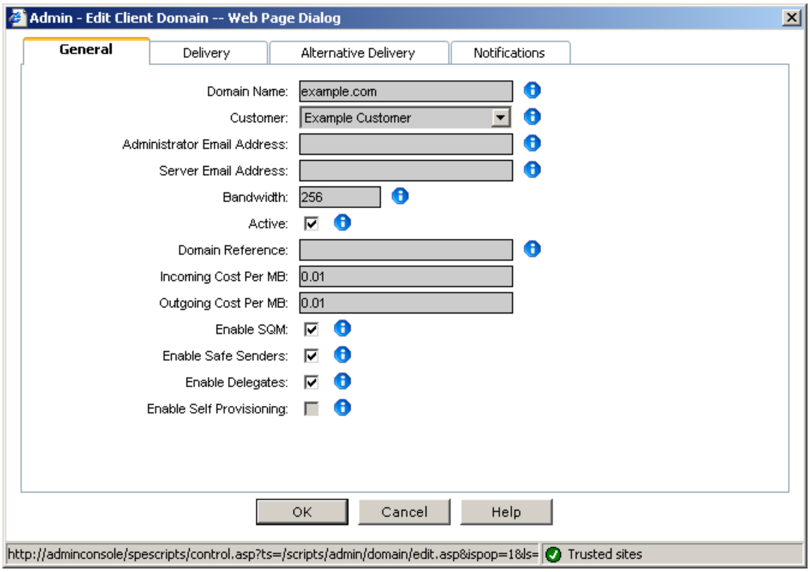
You can configure TLS for delivery of messages from MailMarshal SPE to any customer email domain.

Note: *MailMarshal SPE currently supports TLS for sending only. You cannot configure TLS for mail received by MailMarshal SPE.*

To set up TLS for email outbound to non-customers, see “Advanced Options for Array Properties” on page 92.

To review and configure Domains:

1. In the left pane of the Administration Console, expand the item Client Configuration.
2. Select the Domains item.



Domain Name: example.com
Customer: Example Customer
Administrator Email Address:
Server Email Address:
Bandwidth: 256
Active: ☑
Domain Reference:
Incoming Cost Per MB: 0.01
Outgoing Cost Per MB: 0.01
Enable SQM: ☑
Enable Safe Senders: ☑
Enable Delegates: ☑
Enable Self Provisioning: □

http://adminconsole/spescripts/control.asp?ts=/scripts/admin/domain/edit.asp&ispop=1&ls= Trusted sites

To create or edit a Domain entry:

1. ***If you want to create a new Domain,*** on the main window click **New.**
2. ***If you want to edit an existing Domain,*** on the main window click **Edit.**

Note: *Some settings, including SMTP Authentication, TLS configuration for delivery to the domain, and other minor items, are only available when editing.*

3. On the Domain window, specify the following information:

- **a.** On the General pane, enter the domain name, select the customer to whom this domain belongs, and choose whether the domain is active. Optionally enter administrator and server email addresses specific to this domain.

__Note:__ A new domain is always created as active. You can de-activate a domain, and specify the email addresses, when editing.

- **b.** On the General or Other Settings pane, indicate the bandwidth in KBPS, and enter a reference.

- **c.** On the Delivery pane, enter the server details for the organization's mail server for this domain. When email arrives, MailMarshal SPE will use this delivery information to forward to the Customer's server. ***If you are delivering by IP address,*** enter the IP address of the server. ***If you are delivering by Host Name,*** enter the FQDN of the server.***To authenticate***, check the box and configure required information.

__Note:__ Host Name delivery replaces Dynamic DNS.

- **d.** Optionally select an alternative server (when editing, use the Alternative Delivery tab), and choose whether the second server is used for failover or load balancing.

- **e.** On the Notifications pane, enter the mail queue threshold (email number and waiting time) that is allowed before the Administrator is notified of possible processing errors.

4. ***If you are creating a Domain entry,*** review the previous details by clicking **Back** and **Next** to navigate the wizard. Click **Finish** on the final window to save and close the popup.

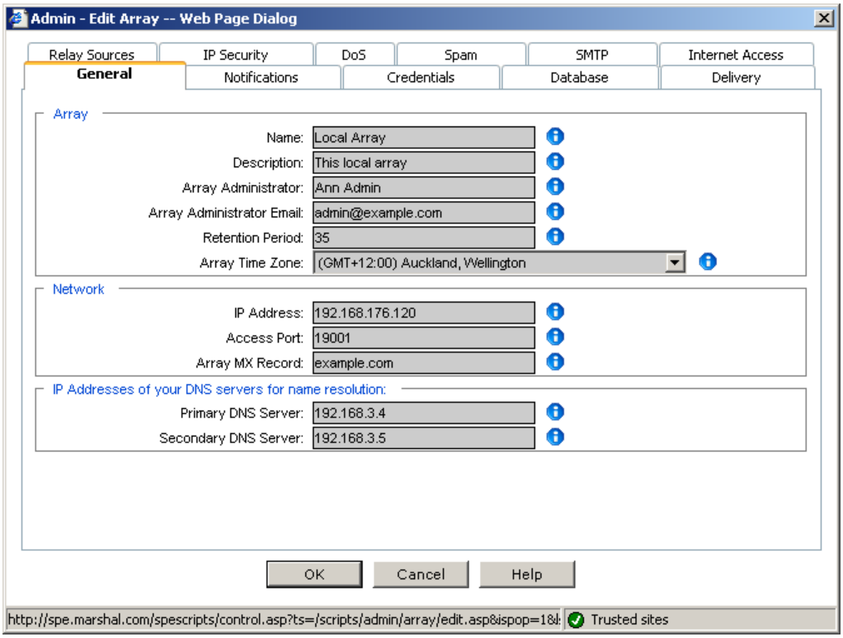
5. ***If you are editing a Domain entry,*** click the respective tabs to review the previous details. Click **OK** to save and close the window.

MANAGING MAILMARSHAL INFRASTRUCTURE

When you install MailMarshal SPE, you configure a list of MailMarshal Array Managers. You may need to update this configuration if you change the MailMarshal SMTP infrastructure, or if you add more MailMarshal SMTP installations.

Note: *Each MailMarshal SMTP installation should be treated as an independent deployment. Each Array Manager will have its own MailMarshal Database, in addition to the MailMarshal SPE database.*

A MailMarshal SMTP Array Manager can include one or more MailMarshal SMTP Email Processing Servers. All customer domains are configured as relay domains. When an email message arrives, it will be processed, then sent to another email server (normally the customer's internal email server) for final delivery.



Array

Name: Local Array

Description: This local array

Array Administrator: Ann Admin

Array Administrator Email: admin@example.com

Retention Period: 35

Array Time Zone: (GMT+12:00) Auckland, Wellington

Network

IP Address: 192.168.176.120

Access Port: 19001

Array MX Record: example.com

IP Addresses of your DNS servers for name resolution:

Primary DNS Server: 192.168.3.4

Secondary DNS Server: 192.168.3.5

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/admin/array/edit.asp&ispop=1&

Configuring Arrays

The Web Administration Console includes extra Array configuration options that allow you to control reload scheduling, relay sources, host security, IP Security, DoS protection and Internet access options.

Many of these options are configured when the Array is created. For more information on the basic options, see "Creating Array Entries" on page 57.

To edit additional Array parameters, double click the array name in the Arrays pane.

***Note:** If you make changes to a MailMarshal SMTP array, after saving the changes you must update the array information in MailMarshal SPE.*

Changes that require an update include:

- *Adding, deleting, or changing an email processing server in a MailMarshal SMTP array. To automatically update the MailMarshal SPE **list of servers** in an array, edit the array in MailMarshal SPE and save it (by clicking **OK**).*
- *Changing IP address, port, or MX records*
- *Changing the MailMarshal SMTP database information. To automatically update the MailMarshal SPE record of the **MailMarshal SMTP database**, edit the array in MailMarshal SPE, display the Credentials tab, and click **Test Credentials**. Then save the array record (by clicking **OK**).*

Notifications

MailMarshal Email Notifications

These addresses are used by automated functions of the MailMarshal SMTP Array Manager. The MailMarshal SMTP Array Manager 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.

The MailMarshal SMTP Array Manager 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.

***Note:** This information is specific to the individual array, and is additional to notifications sent by MailMarshal SPE. These fields are initially populated with the values entered in the MailMarshal SMTP Configuration Wizard.*

SPE Email Notifications (To, From)

Enter email addresses used by the MailMarshal SPE Agent on this array. These values override the values entered in System Settings. For details of fields see **Help**.

Delivery Options

MailMarshal SPE distinguishes between “inbound” and “outbound” email. Inbound email is email delivered to customer organizations. The MailMarshal SMTP Array Manager determines how to deliver this email based on the customer domain information. Outbound email is email delivered to locations outside your local domains. MailMarshal SPE instructs the MailMarshal SMTP servers to deliver this email directly using DNS lookups, or by forwarding all email to a relay host.

1. On the General tab, enter a primary DNS (Domain Name Server) address. Optionally enter a secondary DNS address. Both DNS servers must be able to resolve domain names on the Internet.

Notes: *These DNS servers are used by MailMarshal SMTP processing servers. 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 from the individual email processing servers.*

2. Choose one of the two available delivery options:

   a. **Deliver external email itself:** This is the default option. MailMarshal SMTP processing servers will use DNS resolution to determine the appropriate destination for outbound email and attempt to deliver messages directly. If you select this option, you can optionally enter the name or IP address of a fallback host. The fallback host will be used as a forwarding host for messages that MailMarshal SMTP is unable to deliver immediately. For instance, if MailMarshal SMTP encounters a DNS or greeting failure while attempting to connect to the original destination server it will immediately send the message to the fallback host.

   b. If you want to immediately send all outbound email to a firewall or a fixed relay server, select **Forward email to another SMTP server for delivery.** Enter the host name or IP address of the relay or firewall in the Forwarding Host box. If you want to support host failover or load balancing, enter details of an alternate host.

- If you choose **Fail Over**, MailMarshal SMTP uses the alternate host only when it encounters a DNS or greeting failure while attempting to connect to the main forwarding host.
- If you choose **Load Balance**, MailMarshal SMTP uses both hosts in rotation.

3. To apply the changes, click **OK.**

IP Security

MailMarshal SPE provides configuration settings for anti-relaying, DNS validation (reverse PTR lookup) and Blocked Hosts. This tab allows you to enable or disable these functions.

Note: *To set the servers allowed to relay, see “Setting Relay Sources” on page 90.*

To control how the MailMarshal SMTP servers respond to specific formats of email addresses that can be used to relay email, such as `"user@domain"@domain`, select or clear **Block suspicious local-part relay attempt.** In general you should only clear this box if the customer has a business need to communicate with legacy email servers that use these formats

To permit PTR record host validation, select the **Validate connecting hosts in the DNS** checkbox.

- Choose **Accept unknown hosts** to accept email from hosts without appropriate DNS information, but log this fact to the Windows event log. This option annotates the message header as “not validated”. It is usually used for testing or debugging purposes.
- Choose **Host must have a PTR record** to block messages from any host that does not have a valid DNS PTR record.
- 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.

To enable use of Blocked Hosts, select the **Enable Blocked Host** list checkbox.

For more information, please see “Setting Relay Sources” on page 90 and “Reputation Services” on page 99.

Denial of Service Prevention

Denial of service (DoS) attacks causes target organizations to lose access to common business services, such as email. DoS attacks often involve a high rate of inbound email arriving in a short period of time. In an email DoS attack, the attacker floods email servers with messages, causing the email servers to slow down or cease operation.

You configure DoS attack prevention by specifying the values that the MailMarshal SMTP servers will use when evaluating incoming email traffic. You may need to adjust these values until you determine the optimum settings for your network.

Note: *These settings apply to each MailMarshal processing server separately (not to the array as a whole).*

- Specify the maximum number of connections from a single email server that MailMarshal will accept in any one period (“Evaluation period”).
- Specify the length of Evaluation period MailMarshal considers when deciding whether a remote server is causing a DoS attack. If more than the “Number of connections” is received within an “Evaluation period,” new connections will be refused for the “Blocking Period.”
- Specify the length of Blocking period that MailMarshal refuses messages from an attacking server.
- Optionally enter a list of hosts to exclude from DoS evaluation. See Help for details.

Spam

This tab allows you to specify MailMarshal SpamCensor update information and provides the last update details.

This tab also allows you to enable and configure the SpamProfiler facility that provides signature based spam detection at the Receiver. You can choose to block messages that are identified by SpamProfiler immediately at the SMTP level, or mark them for processing by Standard Rules. You can choose to apply SpamProfiler to inbound messages only, or inbound and outbound messages. You can apply whitelists to bypass SpamProfiler on a per-array basis, and you can apply email users’ Safe Sender lists to SpamProfiler.

Note: *SpamProfiler is optional and licensed separately. SpamProfiler related settings display only if SpamProfiler is licensed. Trial keys support SpamProfiler.*

For details of the fields, see **Help**.

SMTP Settings

The SMTP server settings allow individual MailMarshal SMTP Array Managers to send notification messages. The server specified should be located outside of the MailMarshal SPE architecture, so that notifications can be successfully sent in event of a server failure. These values override the values entered in System Settings. For details of fields see **Help**.

Configuring Internet Access

The MailMarshal SMTP Array Manager requires Web access to download SpamCensor updates. The MailMarshal SMTP processing nodes require Web access to download SpamProfiler updates. If these systems do not have direct access to the Web, you can configure MailMarshal SMTP to use proxy servers. See the **Help** for detailed notes on proxy configuration options.

You can also configure different proxy servers for each node, if necessary. See “Configuring MailMarshal SMTP Entries” on page 59.

Setting Relay Sources

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.

Note: *It is best practice for an email server to refuse relaying requests, unless the source is known and trusted.*

By default, MailMarshal SPE allows relaying requests from the email servers that it delivers local email to for each domain. For instance, if MailMarshal delivers all incoming email for a domain to an Exchange server, MailMarshal will also relay outgoing email from the Exchange server.

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

- By specific account authentication. See “Configuring Accounts” on page 106.
- By setting relaying sources for a customer. See “Configuring Customers” on page 75.
- By IP address range or hostname specific to the Array.

To view relaying permissions for the Array:

1. In the left pane, expand Server Configuration.
2. Click **Arrays** and select an Array. Click **Edit.**
3. Select the **Relay Sources** tab to view the relaying settings for the selected Array.
4. To see the various types of relaying controls, select or clear the **View Domain Relays**, **View Customer Relays**, and **View Array Specific Relays** options.

To permit or deny relaying for the Array:

1. In the left pane, expand Server Configuration.
2. Click **Arrays** and select an Array. Click **Edit.**
3. Select the **Relay Sources** tab to view the relaying settings for the selected Array.
4. To permit or deny relaying from selected locations, edit the list by double clicking the entry. For details of the available options, see Help.
5. To add a new range of addresses, click **New.**

6. To exclude a subset of an allowed range from relaying, enter the subset and clear the Allowed checkbox. For instance, to exclude the 10.2.0.0 subnet from relaying, enter the IP address 10.2.0.0-10.2.255.255, and clear the **Allowed** checkbox.

***Note:** You only need to exclude a range if it is a subset of an included range. Any range that is not explicitly included will be excluded.*

Excluded ranges (denied relaying) are evaluated first. Domain entries are evaluated first, followed by Customer entries and then Array entries.

7. Click **OK** to save and close the Relay Sources entry.

Advanced Options for Array Properties

MailMarshal SPE allows you to configure a number of advanced settings for the selected Array. These settings default to values that are reasonable in the majority of cases. In specific cases you may need to change them.

To work with advanced options for array properties, select **Arrays** in the left pane, select an array in the right pane and then click **Advanced**. For more details about each field, click **Help.**

General

Allows you to configure general behaviors for the array.

- Specify the interval at which services will be polled for monitoring.
- Select a message stamp to notify expired or inactive customers. If MailMarshal does not apply policy to a message because the customer’s trial has expired or the customer is marked inactive, this stamp will be applied to the message.

- Specify a Log Filter regular expression to limit items logged from the MailMarshal SMTP Array Manager service. For more information about LogFilter, see M86 Knowledge Base article Q11915.
- Change the intervals for updates to MailMarshal SPE from the Array Manager, and see when the information was last updated. These include changes to Category Scripts, installed Virus Scanners, and File types.

Note: *MailMarshal SMTP updates this information in real time. These updates only affect the visibility and usability of information in the MailMarshal SPE Web Console.*

Engine

Allows you to set behaviors of the MailMarshal SMTP Engine.

- Specify the number of days for which MailMarshal SMTP Engine logs will be retained.
- Specify the number of messages in the queue that will trigger an email notification.
- Specify the interval for checking of the queue length, in minutes.
- Specify the maximum unpacking depth to determine the number of levels of nested attachments MailMarshal will unpack before quarantining a message as suspicious.
- Specify the maximum MIME nesting depth MailMarshal will unpack before quarantining a message as suspicious.
- Specify RTF Stamping to apply message stamps to Microsoft TNEF/RTF message bodies.
- Specify a Log Filter regular expression to limit items logged from the MailMarshal SMTP Sender service. For more information about LogFilter, see M86 Knowledge Base article Q11915.

Sender

Allows you to set preferences related to the MailMarshal Sender service.

- Specify the number of days for which MailMarshal SMTP Sender logs will be retained.
- Specify the number of messages in the queue that will trigger an email notification and display an abnormal condition in the Dashboard.
- Specify the interval for checking of the queue length, in minutes.
- Specify **Send HELO instead of EHLO** to disable use of extensions to the SMTP protocol when making outbound connections.
- **Deadletter non-returnable messages:** Select this option to determine the disposal of messages that are undeliverable and have no valid return address.
- Specify a Log Filter regular expression to limit items logged from the MailMarshal SMTP Sender service. For more information about LogFilter, see M86 Knowledge Base article Q11915.

Receiver

Allows you to set advanced options related to the MailMarshal Receiver service. The fields are defined as follows:

- Specify the number of days for which MailMarshal SMTP Receiver logs will be retained.
- **Socket time out:** Specifies the period of time that the MailMarshal SMTP receiver waits before dropping a stalled receiver thread.
- **Max inbound recipients per message:** Specifies the maximum number of individual addresses to which an incoming email can be addressed.
- **Max outbound recipients per message:** Specifies the maximum number of individual addresses to which an outgoing email (not addressed to local domains) can be addressed.

- **Greeting string:** Specifies the string MailMarshal sends in response to a connection request. You can include basic variable information in the string.
- **Received header:** Specifies the line that MailMarshal inserts into the header area of each email it receives. You can include basic variable information in the string. Received headers may be used by other email servers processing a message, and this string should only be changed with due care
- **ESMTP Authentication:** Specifies whether MailMarshal advertises that clients can make an authenticated connection. When you enable ESMTP authentication, you can use receiver rules to require authentication. Specify whether authentication is disabled, enabled for all connections including local email servers, or enabled for external connections only.
- **Array Authentication Rule:** Specifies that a default rule allowing SMTP Authentication is written to this array.
- **Reject Unknown Domains:** Specifies that all messages must be addressed to or from a configured customer domain (recommended to prevent relaying of spam in case of misconfiguration at a customer’s server).
- **Bare carriage returns:** Specifies how MailMarshal treats email messages that include a carriage return (CR) character without an accompanying line feed (LF). MailMarshal can ignore the problem and treat the message normally, fix the problem by inserting LF characters, or block the affected messages.
- **Bare line feeds:** Specifies how MailMarshal treats email messages that include a LF character without an accompanying CR. MailMarshal can ignore the problem and treat the message normally, fix the problem by inserting CR characters, or block the affected messages.

Log Filters

Allows you to specify regular expressions to limit items logged from the MailMarshal SMTP services. For more information about LogFilter, see M86 Knowledge Base article Q11915.

Templates

Allows you to select custom templates for MailMarshal SMTP notifications. You can select from existing Message Templates. For more information on creating Message Templates, see “Message Templates and System Templates” on page 131. For more details on selecting templates, see **Help**.

Server Threads

Allows you to specify thread configuration for optimal server performance. For details see **Help**.

Outbound Security (TLS)

Allows you to specify Transport Layer Security settings for sending email from an array to non-customer addresses. For more details, see **Help**

Note: *MailMarshal SPE supports TLS for sending only.*

To set up TLS for sending to a customer’s local domain, see “Setting Up Email Domains” on page 79.

Header Rewrite

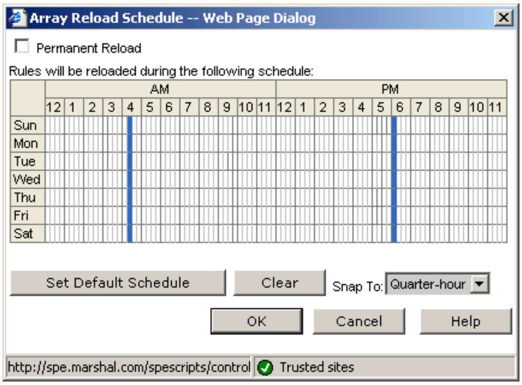
Allows you to specify global Header Rewrite rules for an array. For more details, see Help. For information about the supported syntax, see “Regular Expressions” on page 234.

License Enforcement

Allows you to specify the messages that this array will use to inform users about emails that are not licensed. You can select a message stamp to use when passing through inbound messages. You can select an email template to use for notification when passing through outbound messages. You can enter explanatory text to use when rejecting messages. For more information about the settings see Help. For more information about license enforcement, see “Managing Customer Licenses” on page 74.

Array Reload Schedule

The MailMarshal SPE Replication Agent is responsible for synchronizing settings between the MailMarshal SPE Administration server and the MailMarshal SMTP Array Managers. This option allows you to edit the times when Replication Agent checks for updated information from the MailMarshal SPE Database and starts synchronizing.



Array Reload Schedule -- Web Page Dialog

□ Permanent Reload

Rules will be reloaded during the following schedule:

	AM												PM											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sun					■														■					
Mon					■														■					
Tue					■														■					
Wed					■														■					
Thu					■														■					
Fri					■														■					
Sat					■														■					

Snap To: Quarter-hour

Note:** To order the MailMarshal SPE Replication Agent to synchronize settings immediately (within 90 seconds), navigate to the **Arrays** page, select an array, and then click **Reload.

To set the Array Reload Schedule, select the Array to configure, then click the **Schedule** button.

Alter the schedule block if desired:

- Click on a clear area using the left mouse button to add to the blue “reload” area.
- Click on a blue “reload” area using the left mouse button to erase from the blue “reload” area.

- To reset the schedule to the default time block, click **Set Default Schedule.**
- Choose to “snap” the schedule times to the nearest full, half or quarter hour using the menu.

Normally, synchronization is initiated every 15 minutes. To force MailMarshal SPE to initiate synchronization whenever required, select **Permanent Reload**.

Blocked Hosts

MailMarshal SPE allows you to control acceptance of email messages by checking a list of blocked hosts. You can maintain a list of servers that are never allowed to send any email through each MailMarshal SMTP Array. MailMarshal will reject SMTP connections from these servers.

1. In the left pane, expand Server Configuration.
2. Click Arrays and select an Array.
3. On the main pane, click **Blocked Hosts** to switch to the Blocked Hosts page for the selected Array.
4. To add a new host to block emails, click **New.**
5. In the Blocked Host window, enter an IP address or server name (FQDN) to prevent emails being accepted by MailMarshal.
6. Click **Add** to save and close the entry.
7. To enable checking of the Blocked Host list, enable Blocked Hosts on the **IP Security** tab of the array properties.

Reputation Services

MailMarshal SPE can configure MailMarshal Arrays to retrieve information from DNS based Reputation Services. A Reputation Service is a service that provides an automated response through the DNS protocol (also known as DNS Blacklist or DNS Blocklist). These services typically attempt to list email servers that are associated with spamming, open relays, or other unacceptable behavior.

The Marshal IP Reputation Service is maintained by M86 Security. You can also use services from other vendors, such as Spamhaus. Each list has its own policies, and you should carefully evaluate the lists you choose to use.

You can use Reputation Services for host validation on the array. You can also use Reputation Services in a Receiver rule condition.

Marshal IP Reputation Service

To use the Marshal IP Reputation Service, ensure this feature is included in your MailMarshal SPE license (see the About page of the Console), and ensure that the MailMarshal SMTP Product Key for each array is a valid full key (not a temporary key). To use the service, you will need special credentials tied to the MailMarshal SMTP Product Key. You can retrieve these credentials when adding or editing the service. For more details, see **Help**.

Other Services

To use a Reputation Service from another provider, enter details of the service name and domain in the Reputation Service Properties for each array.,

Warning: *Most Reputation Services require commercial users to pay a fee and/or host a mirror of the lookup zone locally. Carefully review the commercial requirements for each service you intend to use.*

Configuring Reputation Services for an Array

Each Array entry in MailMarshal SPE includes a list of available Reputation Services it can use in Receiver rules.

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

- *You can view the result returned by a Receiver rule in the MailMarshal Receiver text log on the individual processing server.*
- *You can also use Reputation Services in standard rules through the MailMarshal 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 website. You can view the result returned by a Category Script in the message log (if the message is quarantined) or the MailMarshal Engine text log on the individual processing server.*

To configure access to a Reputation Service for a given array:

1. In the left pane, expand Server Configuration.
2. Click **Arrays** and select an Array. On the main pane, click **Reputation Service** to switch to the Reputation Services page for the selected Array.
3. You can edit a service entry or add a new entry. See **Help** for details of the required information.
4. If you want to use a configured list as part of the Adaptive Whitelisting calculation, select the Automatic Adaptive Whitelisting box for the entry
5. Click **OK** to save and close the entry.

Deleting Arrays

If your physical infrastructure changes you may want to delete an array from the MailMarshal SPE installation.

To delete an array:

1. Select the array in the right pane, and then click **Delete**.

Notes: *If only one array is configured and array policies are enabled, you cannot delete the array.*

- *If you delete an array that is hosting customers, as part of the deletion process you can select another array to host these customers.*

Chapter 6
Understanding Email Policy Elements

Email policy elements are building blocks you can use when you create policy groups and rules. These elements help you to specify complex rule conditions and rule actions.

You can edit the existing elements or create new ones to support your policy requirements.

Note: *This section lists all available element types. Some elements may not be available to you because MailMarshal SPE licensing options affect which conditions are available.*

Accounts, Folders, Templates, Message Stamps, Classifications, Header Rewriting, Reputation Services, and User Groups are always available.

- *Anti-Virus: Includes only the basic elements.*
- *Anti-Spam: Includes TextCensors and Digests as well as basic elements.*
- *Content Scanning: Includes all elements.*

For more details of the conditions available under each option, see M86 Knowledge Base article Q12167.

Be aware that MailMarshal SPE does not provide the virus scanner policy element. You must install the scanner software on each email processing server and add the scanners using the MailMarshal Configurator on each Array Manager. MailMarshal SPE polls the Array Managers to determine which scanners are installed. Command line scanners are ***not*** *supported in MailMarshal SPE due to limitations on performance and configuration.*

The following types of elements are available:

Accounts
Allow MailMarshal SMTP email processing servers to authenticate external servers. The accounts can be used to set email relay security on a per customer basis.

External Commands
Allow you to extend MailMarshal SMTP functionality with customized conditions and actions.

Custom File Types
Allow you to extend the library of file types recognized by MailMarshal.

Classifications
Allow you to record the results of MailMarshal evaluation and control the actions that can be taken on a message. You can report on classification actions using Reports.

Classification Groups
Allow you to group classifications for easier reporting.

User Groups
Allow you to apply policy based on email addresses. Groups entered here can be used in Array Policy and customer Packages.

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.

System TextCensors
Allow you to create a source of TextCensor Scripts than can be used by rules without having to duplicate the TextCensor Script for each customer. They can be modified and copied for standard TextCensor Scripts.

Folders
Allow you to create storage locations for messages that have been quarantined, copied or parked by a rule action.

Message Templates

Allow you to notify email users and Administrators about MailMarshal actions, and insert disclaimers and confidentiality statements. You can include specific information about a message using variables.

System Templates

Allow you to create a source of message templates that can be modified and copied for standard message templates.

Message Digests

Allow you to send daily reports on quarantined messages.

Message Stamps

Allow you to add notification text to email messages.

Email Header Matching and Rewriting

Allows you to search for the content of email header fields using Regular Expressions. You can modify, add, or delete headers.

Reputation Services

Allow you to use externally maintained filtering lists that MailMarshal queries by DNS (also known as DNS Blacklists or DNS Blocklists).

To work with policy elements, open the Administration Web Console. In the left pane of the Administration Console select **Policy Elements.**

CONFIGURING ACCOUNTS

MailMarshal accounts consist of a user name and password. You can use accounts to authenticate user connections using a receiver rule. For more information, see “Where sender has authenticated” on page 192.

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, the MailMarshal Arrays using these accounts could become an open relay. Require Customers to change the passwords periodically.*
- *Do not duplicate the credentials of Windows accounts with other permissions. Password transmission during authentication is not strongly secured.*

You must create an Array Authentication rule for authentication to work reliably. See the Receiver section in “Advanced Options for Array Properties” on page 92.

To create or edit accounts:

1. In the left pane of the Administration Web Console, expand **Policy Elements > Accounts**.
2. ***If you want to create a new Account,*** on the main window click **New.**
3. ***If you want to edit an existing Account,*** on the main window select the item and then click **Edit.**
4. On the Account window:
   - **a.** Specify the account name and password to authenticate the account.
   - **b.** Select the Array that this account should be created on.
5. Click **OK** to save changes.

CONFIGURING EXTERNAL COMMANDS

An external command is a custom executable, Windows command, or batch file that can be run by a MailMarshal SMTP email processing server. 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.” If you want to use an external command to check for a condition, the command must return a standard return code.

Note: *The External Command rule condition and action are only available in Array Policies. They are not available in Customer Packages or Advanced Customer policies.*

You can also use custom executable files with the standard rule action “Run the external command.”

MailMarshal SPE is provided by default with the external command for message release that is standard to MailMarshal SMTP. For more information about this command, see “Using the Message Release External Command” on page 214.

To use an external command in MailMarshal SPE rules, you must first define it.

To create a new external command definition:

1. In the left pane of the Administration Web Console, expand **Policy Elements > External Commands**.
2. ***If you want to create a new external command definition,*** on the main window click **New.**
3. ***If you want to edit an existing definition,*** on the main window select the item and then click **Edit.**

4. Enter a name for the external command.

5. Type the name of the executable file. You can also browse for the file by clicking **Browse**.

Note: *You must place the file in the* `\config` *folder on each MailMarshal SMTP Array Manager on the arrays where you plan to use this command. The file will be replicated to all processing nodes*

6. 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 variables.

7. The **Timeout** and **Timeout per MB** values control how long MailMarshal 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 will terminate the command, log the event as a runaway process, and place the message in the Dead Letter\Unpacking folder.*

8. 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.

9. 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 want to parse attached files, clear this box to apply the command to every attachment.

10. 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 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 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 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 CUSTOM FILE TYPES

Custom File Types allow you to extend the library of file types recognized by MailMarshal. MailMarshal recognizes many, but not all, executable, image, document, movie, sound, archive, encrypted, and other file types. If MailMarshal does not recognize an attachment as a legitimate file type during mail processing, it tags the unrecognized file as Binary Unknown (BIN). You can add a custom file type definition locally. Once MailMarshal recognizes the file as a custom file type, and not as BIN, the attachment will not trigger a Block Unknown Attachments rule.

For details of the custom file type syntax and hints about creating custom type definitions, see M86 Knowledge Base article Q10199.

Note: *When you add or change custom file types, they may not be visible in the Rule Wizard for 5 minutes or longer. Allow a full replication cycle before using the types in rules. All arrays and servers should show “up to date.” Depending on the size of the configuration and network issues, this could be 15 minutes or more.*

Working with Custom File Types

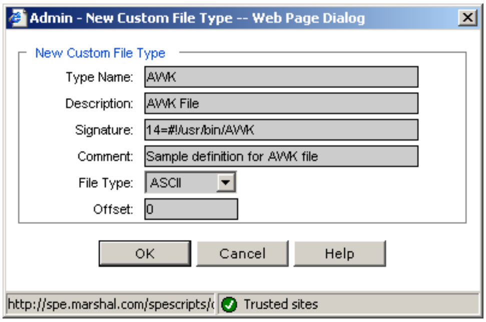
To add a custom file type:

1. In the left pane of the Administration Web Console, expand **Policy Elements > Custom File Types.**
2. Click **New.**
3. Enter the required information. Note that the fields map to the custom type file as follows:
   - Type Name (T)
   - Description (D)
   - Signature (second part of data)

     -For File Type Ascii, the format is `length=ascii signature`

     -for File Type Binary, the format is `hexadecimal signature`
   - Comment (#)
   - File Type (Ascii=A; Binary=X)
   - Offset (first part of data of entry A or X)

   For example, the following data entry corresponds to the file lines shown:



Admin - New Custom File Type -- Web Page Dialog

New Custom File Type

Type Name: AWK

Description: AWK File

Signature: 14=#!/usr/bin/AWK

Comment: Sample definition for AWK file

File Type: ASCII

Offset: 0

```
T:AWK
D:AWK File
A:0,14=#!/usr/bin/AWK
#:Sample definition for AWK file
```

4. Click **OK.**

To edit a custom file type:

1. In the left pane of the Administration Web Console, expand **Policy Elements > Custom File Types.**
2. Select an entry, and then click **Edit.**
3. Edit the information, and then click **OK.**

To delete a custom file type:

1. In the left pane of the Administration Web Console, expand **Policy Elements > Custom File Types.**
2. Select a type entry.
3. Click **Delete.**

USING MESSAGE CLASSIFICATIONS AND CLASSIFICATION GROUPS

MailMarshal SPE uses message classifications as the main method of searching for messages and setting permissions for users to process messages. A large number of classifications are included by default.

You can use classifications to give additional granularity for searching and reporting. Classifications also determine what messages are visible to users in the SQM for self management.

Classification Groups are used to simplify reporting on multiple classifications.

Working With Message Classifications

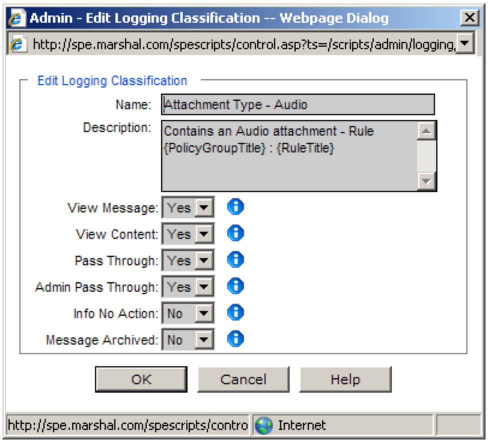
To work with Message Classifications in the Administration Console, select Classifications from the left pane menu tree.

To create a message classification:

1. In the left pane of the Administration Console, expand **Policy Elements > Classifications.**
2. Click **New.**
3. In the window, enter a meaningful name for the classification.
4. 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.
5. Choose additional settings that apply to messages in this classification. Select one or more of the following:
    - **View message:** Users can view the message
    - **Pass through message:** Users can release the message to its destination
    - **Administrator pass through message:** Administrative users can view the message
    - **Info only:** The classification is only for information. The message was not quarantined.
    - **Message archived:** The message is archived and cannot be deleted.
    - **SQM Default:** The classification will be added to the list of classifications visible in the SQM for all new customers. When you apply this setting you can also specify that the classification should be added to the SQM for all existing customers.
6. To add the classification, click **OK**.

Editing Message Classifications

You can edit the name and description of a classification.



Admin - Edit Logging Classification -- Webpage Dialog
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/admin/logging,
Edit Logging Classification
OK
Cancel
Help
http://spe.marshal.com/spescripts/contro
Internet

Name: Attachment Type - Audio

Description: Contains an Audio attachment - Rule {PolicyGroupTitle} : {RuleTitle}

View Message: Yes

View Content: Yes

Pass Through: Yes

Admin Pass Through: Yes

Info No Action: No

Message Archived: No

To edit a message classification:

1. Double-click the classification name in the right pane of the Administration Console to view its properties.
2. Make any required changes.
3. Click **OK.**

Disabling and Enabling Message Classifications

You can disable or enable a classification to control its use in new Rules. Disabled classifications are displayed in a separate tab.

To disable a message classification:

1. Select the classification name in the Administration Console.
2. Click **Disable**.

To enable a message classification:

1. Select the classification name in the Administration Console (on the Disabled tab of the Classifications window.
2. Click **Enable**.

Deleting Message Classifications

You can delete a classification if it is not used in any rules. Deleted classifications are displayed in a separate tab and can be undeleted if required.

To delete a message classification:

1. Select the classification name in the right pane of the Administration Console.
2. Click **Delete**.

Working With Classification Groups

To work with Message Classifications in the Administration Console, select Classification Groups from the left pane menu tree.

To create a classification group:

1. In the left pane of the Administration Console, expand **Policy Elements > Classification Groups.**
2. Click **New.**
3. In the window, enter a meaningful name for the classification group.
4. Give a brief description of the group and its purpose. This description will be used in the Console and Reports.
5. Click **OK**.

Editing Classification Group Membership

You can add or remove classifications from a group.

To add a classification to a group:

1. Select the group in the left pane of the Administration Web Console.
2. Click **Add.**
3. Select a classification to add, and then click **OK**.

To remove a classification from a group:

1. Select the group in the left pane of the Administration Web Console.
2. Select the classification you want to remove.
3. Click **Remove.**

Editing Classification Groups

You can edit the name and description of a classification group.

To edit a classification group:

1. Double-click the classification group name in the right pane of the Administration Console to view its properties.
2. Make any required changes.
3. Click **OK.**

Deleting Classification Groups

You can delete a classification group.

To delete a classification group:

1. Select the group name in the right pane of the Administration Console.
2. Click **Delete**.

CONFIGURING USER GROUPS

User groups allow you to apply policy to specific users (such as departments within a customer organization). MailMarshal uses SMTP email addresses to perform user matching. You can create and populate user groups within MailMarshal SPE by entering email addresses manually or copying them from other Groups. You can use wildcard characters when you define groups. You can import and export user groups with text files.

You can create User Groups from the Administration Web Console. These Groups can be used in Array Policy and Customer Package rules.

Customers can create User Groups in the Customer Web console. They can use these groups in rules they create. You can also allow customers to import user groups from LDAP or Active Directory with the SPE Connector Agent. For details of the Connector Agent, see the *User Guide.*

User Group Types

MailMarshal SPE allows two types of user groups - Internal and External.

- An Internal user group contains only email addresses within customer organizations, such as `john.s@xyz.com`.
- An External user group contains only addresses that are not managed by the Service Provider, such as `trusted@example.com`
- A group imported through the Connector Agent displays as type LDAP. The group is treated as Internal.

***Note:** MailMarshal SPE does not enforce domain restrictions on email addresses you create in the Administration Web Console. Enter addresses or patterns carefully to avoid unexpected results.*

Rule User Matching can only select user groups as per the table below:

	Incoming Rules	**Outgoing Rules**
Addressed From	External Groups	Internal Groups
Addressed To	Internal Groups	External Groups

Creating and Populating User Groups

To create a user group:

1. In the left pane of the Administration Web Console, expand **Policy Elements > User Groups.**
2. On the main window, click **New**.
3. Choose **New** to create a user group.
4. On the User Groups window:
   a. Enter a group name for the group, and specify whether the group will contain Internal or External email addresses.
   b. Optionally specify Incoming and Outgoing Cost per MB for reporting purposes.
5. When you have entered all the required information, click **OK**.

Adding Members to a MailMarshal SPE Group

You can add addresses or wildcard patterns to a MailMarshal SPE user group, and you can insert other groups. You can also import users from a text file.

To add members to a user group:

1. Select the appropriate user group by expanding the user group name from **Policy Elements > User Groups** on the Administration Console's left pane. Alternatively, select the User group name from Policy Elements, then click **Members.**
2. To add an individual address or wildcard pattern, click **New.** In the New User window, enter an individual SMTP address, a partial address using wildcard characters, or a domain name, and then click **Add.** The value is added and a new window opens so you can enter additional values.

3. To insert another group, click Insert User Group. In the new window, select a group from the list, and then click Add.

4. When you have completed entry of all addresses, click **OK.**

To import members from a simple text file to a MailMarshal SPE user group:

1. Select the appropriate user group by expanding the usergroup name from **Policy Elements > User Groups** on the Administration Console's left pane.

2. On the main window, click **Import.**

3. In the Import User List window, select the local file you wish to upload, and click **Import** to proceed.

Notes: *The file must contain one email address per line.*

- *Importing removes any existing addresses from the group.*
- *Included groups are not removed and cannot be imported.*

To export members of a MailMarshal SPE user group:

1. Select the appropriate user group by expanding the usergroup name from **Policy Elements > User Groups** on the Administration Console's left pane.

2. On the main window, click **Export.**

3. In the Export User List window, click the link to export. Save the file using your browser’s file download dialog. In the Export User List window, click **Close.**

Note: *Included groups are not exported.*

Identifying Email Text Content Using TextCensor Scripts

TextCensor scripts check for the presence of particular lexical (text) content in an email message. MailMarshal 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 SPE Web Console 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. You should also caution customers about this content.*

MailMarshal SPE Administration Console provides two types of TextCensor script available in the Administration Console.

TextCensor Scripts
Used by MailMarshal to apply text checks while processing email.

System TextCensors
Model scripts made available as the starting point for customizations, and also available for selection when creating rule conditions.

Both types of scripts are created the same way.

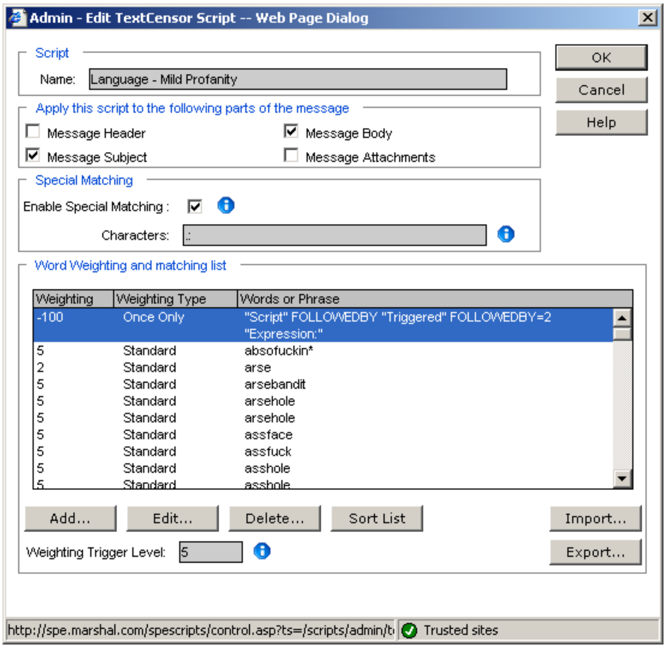
Creating Scripts

To work with TextCensor Scripts, select **Policy Elements > TextCensors** in the left pane of the Administration Console.

To add a TextCensor Script:

1. In the left pane of the Administration Console, expand **TextCensor Scripts** or **System TextCensors.**
2. On the main pane, choose **New TextCensor Script** to open the TextCensor Script window
3. Enter a name for the script.
4. Choose a previous model to base the new TextCensor on. For instance, you may want to start with a Blank template or from a System TextCensor such as one which deals with Pornographic language.

5. Click **OK** to edit the TextCensor details.



Script

Name: Language - Mild Profanity

Apply this script to the following parts of the message

☐ Message Header ☑ Message Body

☑ Message Subject ☐ Message Attachments

Special Matching

Enable Special Matching : ☑

Characters: :

Word Weighting and matching list

Weighting	Weighting Type	Words or Phrase
-100	Once Only	"Script" FOLLOWEDBY "Triggered" FOLLOWEDBY=2 "Expression:"
5	Standard	absofuckin*
2	Standard	arse
5	Standard	arsebandit
5	Standard	arsehole
5	Standard	arsehole
5	Standard	assface
5	Standard	assfuck
5	Standard	asshole
5	Standard	asshole

Weighting Trigger Level: 5

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/admin/t Trusted sites

6. On the TextCensor details window, 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.

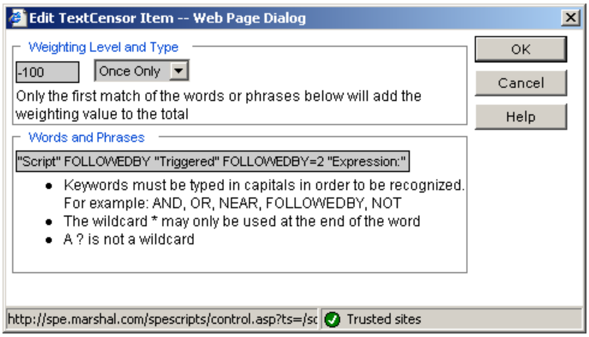
Note: *The script will check each part separately.*

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.

7. 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 `<script` 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: "=".*

8. Add one or more TextCensor items. To begin adding items, in the TextCensor Script window click **Add** to open the TextCensor Item window**.**



Edit TextCensor Item -- Web Page Dialog

Weighting Level and Type

-100 Once Only

Only the first match of the words or phrases below will add the weighting value to the total

Words and Phrases

"Script" FOLLOWEDBY "Triggered" FOLLOWEDBY=2 "Expression:"

- Keywords must be typed in capitals in order to be recognized. For example: AND, OR, NEAR, FOLLOWEDBY, NOT
- The wildcard * may only be used at the end of the word
- A ? is not a wildcard

http://spe.marshal.com/spescripts/control.asp?ts=/sc Trusted sites

9. Select a weighting level and type for the item. For more information, see "Script and Item Weighting" on page 125.

10. 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.*

11. To add the value to this script, click **OK**.
12. When you have entered all items, click **Finish** to return to the New TextCensor Script window.
13. 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.
14. 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 main pane.
2. Edit an item by double-clicking it.
3. Delete an item by selecting it 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. Click **Sort List** 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. Select the TextCensor on the main pane.
2. Click **Duplicate** on the 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 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* ***Sort List*** *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)

Operator	Function	Example
NOT	Logical negation of terms; use after other operators; means “anything else but.”	Dog AND NOT cat Dog FOLLOWEDBY (NOT house)
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

Importing Scripts

You can import scripts in files. Use this function to copy a script from another MailMarshal installation, or to restore a backup.

Note: *If you import a script into an existing script, all existing information will be overwritten.*

To import a TextCensor Script from an XML file:

1. Create a new TextCensor.
2. Click **Import**.
3. Choose the file to import from, and click **Open.**
4. In the New or Edit TextCensor Script window, click **OK** or **Finish**.

Exporting Scripts

You can save scripts in files. Use this function to back up a script, or to edit a script in another application such as Microsoft Excel.

To export a TextCensor Script to an XML file:

1. Double-click the name of the script to be exported in the right pane to bring up the Edit TextCensor Script window.
2. Click **Export.**
3. Click **Click here to download the TextCensor**, then enter the name of the file to export to.
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 applies TextCensor scripts to text portions of messages. Depending on the potions you select, a script can apply to headers, message bodies, and attachment content. MailMarshal 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.

NOTIFYING USERS WITH MESSAGE TEMPLATES

MailMarshal SPE 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 has modified it.

Message templates are complete email messages that can be sent to a user or Administrator. MailMarshal uses templates for system notifications such as non-delivery reports. You can also use them to provide auto-responders or other custom notices. MailMarshal SPE can use special digest templates to provide users with summary information about quarantined email.

MailMarshal SPE Administration Console provides two types of Template available in the Administration Console.

Message Templates
Used to notify users or administrators about MailMarshal actions while processing email.

System Templates
Model templates made available as the starting point for customizations, but not available for selection in rule conditions.

Both types of templates are created the same way.

MailMarshal 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 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 has taken on a specific message.

Message Templates and System Templates

Message templates are used when MailMarshal 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.

The same rule can send several notification messages. For instance, if MailMarshal 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 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 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.

System Templates are pre-configured templates that Administrators and customers can use as models when creating new templates. Administrators can create, edit and delete System Templates.

Note: *In addition to rule notification templates, MailMarshal uses a number of pre-configured templates for administrative notifications (such as delivery failure notifications). These templates are configured in the advanced properties of each array. All Message Templates can be used for administrative notifications.*

Creating a Message Template

To work with templates, select **Message Templates** or **System Templates** in the left pane of the Administration Console.

To create a message template:

1. In the left pane of the Administration Console, select **Policy Elements > Message Templates** or **Policy Elements > System Templates.**
2. On the main window, select **New** to open the Message Template window.
3. Enter a name for the Template, and select the type Message Template. Choose a previous model to base the new Template with. For instance, you may want to start with a Blank template or from a System Template such as one which deals with Delayed Emails.

4. Click **OK** to edit the Template details.
5. By default, MailMarshal SPE shows the HTML message body. To enable the plain text body or edit both types separately, click the Options tab.
6. To see additional address fields, click the **Options** tab.
7. 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.
8. Enter text in the body section.
9. Click **Finish** to return to the message template window.

When creating templates, you can use variables marked with braces { }. You can use nested variables. For details of the variables available in templates, see “Using Variables” on page 144.

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.*

From the Options tab, you can attach files to the notification, including the original message, or the MailMarshal message processing log

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 138.

Digest templates are similar to message templates. The key differences are:

- You cannot attach files, messages, or message logs to digest templates.
- You cannot use the CC and BCC fields.
- You cannot create a blank Digest Template.

- You must associate each digest template with a message digest.

Digest templates support variables specific to the digesting function that are not available in message templates. These variables allow MailMarshal 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).
NORELEASE	Do not show the message release links.
RELEASEURL=*url*	Specify the URL path to the Release webpage used for this digest (see example below). Defaults to the URL configured on the Global tab of System Settings. This option is unlikely to be required in MailMarshal SPE.
GROUP	Group entries by folder, for digests covering multiple folders.
SHOWFROM= *yes|no*	Show the sender address. Defaults to yes.

Option	Results
SHOWTO=*yes*|*no*	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}
```

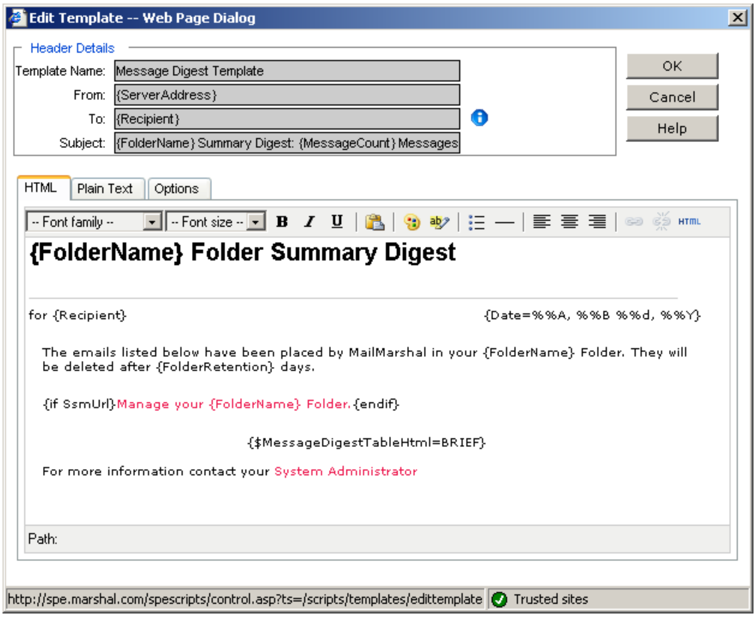
For details of other variables available in digest templates, see "Using Variables" on page 144.

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 Administration Console, select **Policy Elements > Message Templates** or **Policy Elements > System Templates.**
2. On the main window, select **New** to open the Message Template window.
3. Enter a name for the Template, and select the type Message Digest. Choose a previous model to base the new Template with. For instance, you may want to start with a Blank template or a Compact Digest.

4. Click **OK** to edit the Template details.



Template Name: Message Digest Template

From: {ServerAddress}

To: {Recipient}

Subject: {FolderName} Summary Digest: {MessageCount} Messages

{FolderName} Folder Summary Digest

for {Recipient} {Date=%%A, %%B %%d, %%Y}

The emails listed below have been placed by MailMarshal in your {FolderName} Folder. They will be deleted after {FolderRetention} days.

{if SsmUrl}Manage your {FolderName} Folder.{endif}

{$MessageDigestTableHtml=BRIEF}

For more information contact your System Administrator

Path:

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/templates/edittemplate Trusted sites

5. By default, MailMarshal SPE shows the HTML message body. To enable the plain text body or edit both types separately, click the Options tab.

6. To see additional address fields, click the **Options** tab.

7. 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.

8. Enter text in the body section.

9. Click **Finish** to return to the message template window.

10. You can use variables marked with braces { }. For details of the variables available in templates, see “Using Variables” on page 144. The Message Digest Template variables are required in Digest Templates.

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 main window of the Administration Console.
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. Select a template name on the main pane of the Administration Console.
2. Click **Duplicate**.
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 name on the main pane of the Administration Console.
2. Click **Delete**.

SETTING UP MESSAGE DIGESTS

MailMarshal allows you to send email summaries to users, notifying them about messages MailMarshal has quarantined. Users can review and release the messages directly from the digest email. 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
- Provide a list of Dead Letter email
- Include messages with specific classifications (not available for Dead Letter folders)
- 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 133.
- Send digest emails to each user with undigested email in the folder, or send all digest emails to a specified address

To work with message digests in the Administrator Web Console, select **Policy Elements > 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 and user group 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 right pane of the Web Console, click **New** to start the New Message Digest Wizard.
2. On the General window, give the Digest a name and specify the template to use when generating the email. Optionally select **Send all digest notifications to** if you want to deliver all results of this digest to the same address (for instance, if you are digesting Dead Letters for multiple customers).
3. On the folders window, choose one or more folders to digest.

***Note:** You cannot include both Dead Letter and Quarantine folders in the same Digest.*

4. On the Classifications window, choose one or more classifications to limit the digest. You must select at least one classification.

***Note:** This window does not display if you selected a Dead Letter folder in the previous step. Dead Letters do not have multiple classifications.*

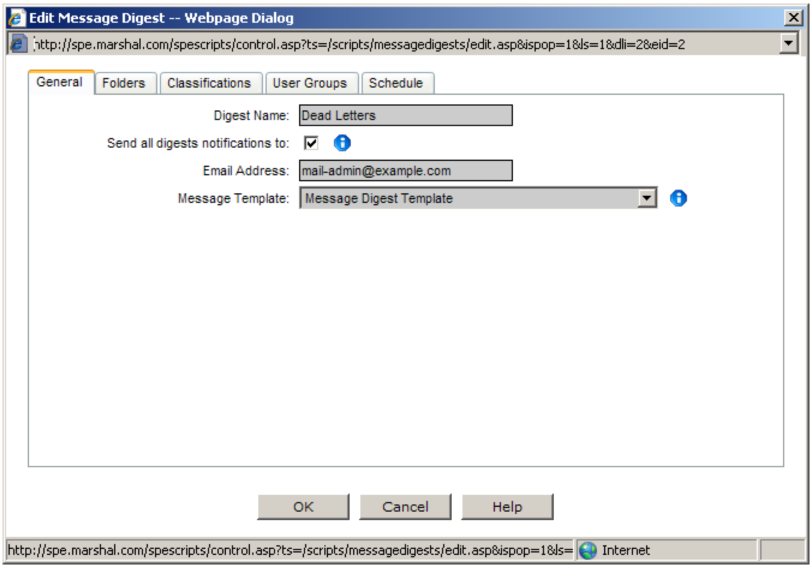
5. On the Schedule window, select a time and one or more days when the digest will be created. The schedule is repeated weekly.
6. Click **Finish.**

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 Web Console 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.**



http://spe.marshal.com/spescripts/control.asp?ts=/scripts/messagedigests/edit.asp&ispop=1&ls=1&dli=2&eid=2

Digest Name: Dead Letters

Send all digests notifications to: ☑

Email Address: mail-admin@example.com

Message Template: Message Digest Template

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/messagedigests/edit.asp&ispop=1&ls=

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 Web Console.
2. Click the **Delete** button.

NOTIFYING USERS WITH MESSAGE STAMPS

Message stamps are short blocks of text that MailMarshal can apply to the top or bottom of an email message body. MailMarshal message stamps can include a plain text and an HTML version. MailMarshal 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 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 Administration Console, select **Message Stamps** in the left pane.

Creating Message Stamps

To create a message stamp:

1. In the left pane of the Administration Web Console, select **Policy Elements > Message Stamps.**
2. On the main pane, click **New.**
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.

Note: *If message stamping is enabled for RTF (Microsoft TNEF) messages, the plain text message stamp will be used for these messages. RTF stamping is enabled by default. To enable or disable RTF stamping, see the Engine tab of Advanced Array settings for each array.*

7. To add the new stamp to the list of available message stamps, click **OK**

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. On the main pane, select a message stamp.
2. Click **Duplicate**.
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. On the main pane, select a message stamp.
2. Click **Edit**.
3. Make the required changes.
4. 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. On the main pane, select a message stamp.
2. Click **Delete**.

Using Variables

When you create a message template, digest template, message stamp, or message classification description, you can use a number of variables. MailMarshal substitutes the appropriate information when it uses the template or stamp.

Variables are marked by curly braces { }.

Not all variables are available in all contexts. MailMarshal may not have the required information to substitute. If MailMarshal 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
{$MessageDigestTableHTML *=detail[,option,option,...]*}	The HTML version of a message digest detail listing. For full information about options, see "Creating Digest Templates" on page 133. See also the variable {MessageDigestTableText}.
{Administrator}	Email address of the Administrator as set during post-installation configuration and accessible from the General tab of the Array Properties.
{AdministratorAddressRecipient}	Email address of the administrator for the recipient customer domain.
{AdministratorAddressSender}	Email address of the administrator for the sender customer domain.
{ArrivalTime}	The time when MailMarshal received a message.
{AttachmentName}	File name of the attached file that triggered a rule condition.
{Date}	The current date. For more information, see "Date Formatting" on page 149.
{DateLastRun}	The date of the previous MailMarshal message digest for a folder.

Variable	Data inserted
{Errorlevel}	The last error returned by a virus scanner.
{Env=*varname*}	Inserts the value of a Windows environment variable.
{ExternalCommand}	The name of the last External Command used.
{ExternalSender}	Returns 'y' or 'n' depending on whether the sender was outside or inside the “allowed to relay” space.
{File=*fullpath*}	Inserts a text file within the body of a message (for instance, can be used to insert the MailMarshal log for a message in a notification email body).
{Folder}	The name of the folder that is the subject of a MailMarshal message digest email.
{Folder Retention}	The retention period for a folder that is the subject of a MailMarshal message digest email.
{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 received this message.
{If *variable*}...[{else}...]{endif}	Allows conditional substitution of text. The condition is true if the variable is not empty. For example: `{If VirusName}This message contained the virus {VirusName}.{endif}` The Else clause is optional.
{InitialMessageBody}	The first 200 characters of the body of the message.
{Install}	The install location of MailMarshal.

Variable	Data inserted
{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.
{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}. **Note:** 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}	**Note:** 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.

Variable	Data inserted
{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 214.
{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 214.
{ReplyTo}	Email address in the 'Reply to' field of the message.
{RemoteIP}	The IP of the remote machine.
{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.

Variable	Data inserted
{ServerAddress}	Email address used as the 'From' address for notifications as set during post-installation configuration and accessible from the Notifications tab of Array Properties.
{ServerAddressRecipient}	Email address used as the ‘From’ address for notifications from the recipient customer domain.
{ServerAddressSender}	Email address used as the ‘From’ address for notifications from the sender customer domain.
{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)
{Ssmurl}	The URL of the End User Management (SQM) website, as entered in System Settings. Used by the digest templates.
{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 working folder name.
{Time}	The current time. See also “Date Formatting” on page 149.
{TimeEnteredQueue}	The time that the message entered the MailMarshal Queue.
{TimeLeft}	The time left to attempt delivering the message in question.

Variable	Data inserted
{UnsubscribeUrl}	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: `{if UnsubscribeUrl}To unsubscribe from this digest, use the following link: {UnsubscribeUrl} {endif}`
{VirusName}	Name of the virus detected. This information is provided by all DLL based scanners supported in MailMarshal SPE.
{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`.

***Note:** Each sub-variable must be preceded by %%. For example, to ensure that the date is formatted according to the Windows locale, use {date=%%c}.*

The following table lists the available date formatting sub-variables:

Variable	Value inserted
a	Abbreviated weekday name
A	Full weekday name

Variable	Value inserted
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)
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 EMAIL FOLDERS

MailMarshal 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.

Each MailMarshal SPE folder is used for either inbound or outbound messages, but not both.

MailMarshal SPE includes a number of predefined folders for the system, and a separate set of predefined folders for each customer. These folders include:

- Archive Incoming
- Archive Outgoing
- Parking Incoming
- Parking Outgoing
- Quarantine Incoming
- Quarantine Outgoing

Note: *Customers can only use the default folders for their company when creating rules. You can allow customers to produce digests of global folders.*

Working with folders

You can create new folders that will be available for use in Array Policy and Customer Packages.

Predefined and newly-created folders have default properties that you can modify. For instance, by default MailMarshal saves messages stored in the folder for a specific period of time. The defaults and the available options depend on the type of folder.

Note: *You can determine the processing options for a message released from a folder, using the rule action that places the message in the folder. See "Copy the message to folder with release action" on page 197 and "Move the Message to folder with release action" on page 201.*

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.

Archive folder
Used to keep historic copies of delivered mail. You cannot manually delete mail stored in an archive folder.

Parking folder
Used to delay the delivery of mail. MailMarshal releases messages stored in the folder according to a configurable schedule associated with the folder.

To create a folder:

1. In the left pane of the Administration Console, expand **Policy Elements > Folders.**
2. Click **New.**
3. Specify the appropriate values. For more information about fields on a window, click **Help**.
4. Click **OK.**

Editing folders

You can change the name and most features of a folder. You cannot change the type or processing direction of an existing folder.

To edit a folder:

1. In the left pane of the Administration Console, expand **Policy Elements > Folders.**
2. Select the folder you want to modify.
3. Click **Edit**.
4. 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 Administration Console, select the folder name.
2. Click **Delete**.

Deleting a folder in the Administration Console does not delete the physical folder or any email messages it contains.

HEADER MATCHING AND REWRITING

MailMarshal SPE 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. Advanced customers can use header searches only.

⚠ ***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 SPE 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 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. In the Administrative Web Console, select **Server Configuration > Arrays.**
2. On the Array Advanced Properties window, click the Header Rewrite tab. From this tab 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.

Note: *You must set up global header rewriting separately for each array in the MailMarshal SPE installation.*

For details of the rule editing processes, see “Using the Header Rewrite Wizard” on page 156.

Using Rules to Find Headers

You can search email headers using regular expressions using the MailMarshal SPE 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 156.

Using Rules to Change Headers

You can alter email headers using regular expressions using the MailMarshal SPE 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 234.

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.

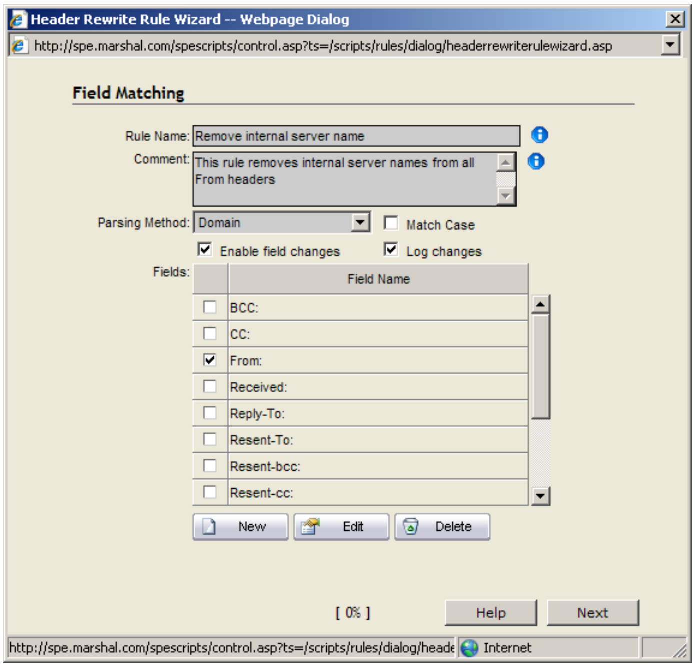
To use the Header Wizard:

1. Enter a name and optional comment for the rule.
2. Choose a parsing method from the list. Depending on this selection, MailMarshal SPE will apply regular expression matching to parts or all of the selected headers.
    - If you select the method “Entire Line” MailMarshal SPE will use the entire text of the header as the input text for the substitution engine.
    - If you select the method “Email Address” MailMarshal SPE will use each email address found in the line as the input text.
    - If you select the method “Domain” MailMarshal SPE 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. ***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 SPE logs for the message. If only **Log changes** is selected, the logs will show the changes that would have occurred.

5. 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.



Header Rewrite Rule Wizard -- Webpage Dialog

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/headerrewriterulewizard.asp

Field Matching

Rule Name: Remove internal server name

Comment: This rule removes internal server names from all From headers

Parsing Method: Domain

□ Match Case

☑ Enable field changes

☑ Log changes

Fields:

	Field Name
□	BCC:
□	CC:
☑	From:
□	Received:
□	Reply-To:
□	Resent-To:
□	Resent-bcc:
□	Resent-cc:

New
Edit
Delete
[0%]
Help
Next
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/heade
Internet

6. Click **Next** to proceed to the Field Search window (matching rules) or the Field Substitution window (rewriting rules).

7. 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 “exclusion matched” (the rule will not be triggered).

8. In the **Field Search Expression** field, enter a regular expression that MailMarshal SPE should use to select the data for matching. If the input text matches this expression, the rule will match it, subject to exceptions based on the exclusion filter.

9. ***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.

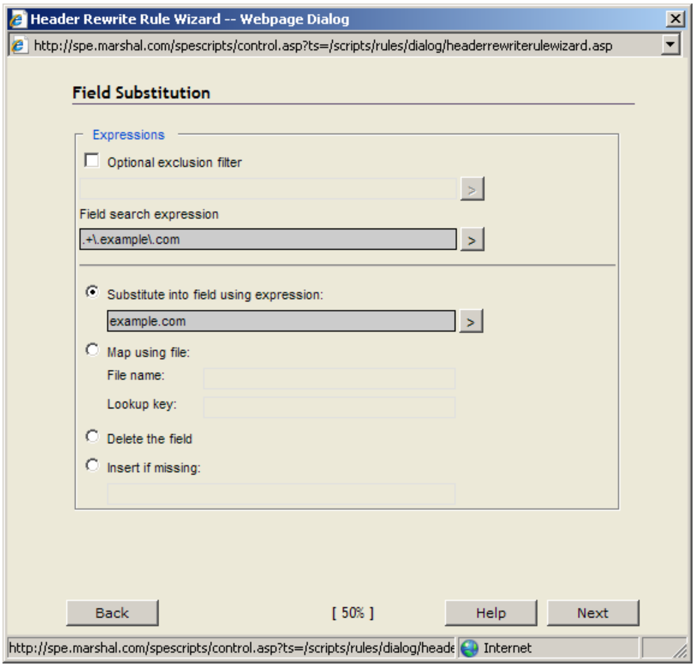
Note: *If you replace the entire contents of a field, be sure to terminate the text with a CRLF (\r\n). You can insert this value through the arrow to the right of the field. If you enter $0 (the tagged expression containing the entire input line) at the end of the substitution expression, a CRLF will 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. For more information about map file usage, see “Map Files” on page 238.

Note: *You must manually place the file in the* `config` *subfolder of the MailMarshal SMTP installation folder on each Array Manager. If the file is not present in this location, the rule will not be written to the array.*

- **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.

10. **Insert if missing** permits you to add a new header if any of the selected headers does not exist. MailMarshal SPE 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.`



Header Rewrite Rule Wizard -- Webpage Dialog

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/headerrewriterulewizard.asp

Field Substitution

Expressions

□ Optional exclusion filter

Field search expression

.+\.example\.com

● Substitute into field using expression:

example.com

○ Map using file:

File name:

Lookup key:

○ Delete the field

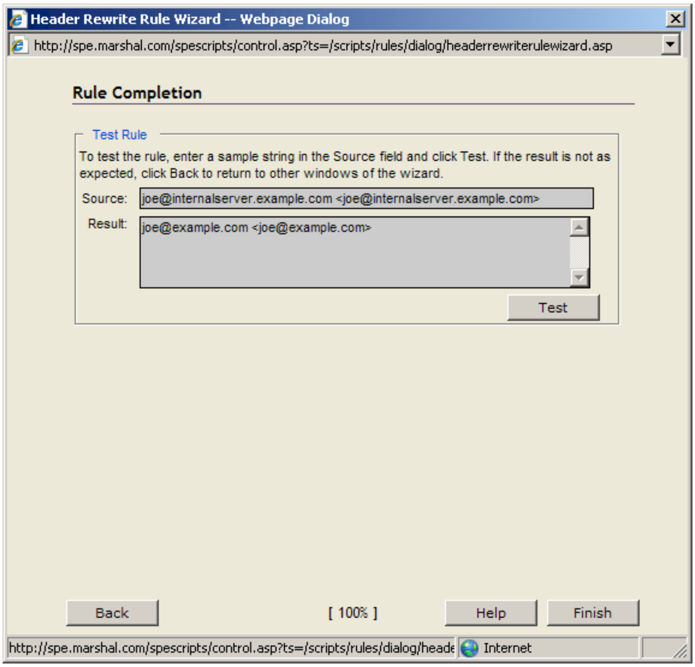
○ Insert if missing:

Back
[50%]
Help
Next
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/heade
Internet

11. ***If this is a rewriting rule,*** click **Next** to proceed to the Rule Completion window.

12. To test the rule, enter an input string in the **Source** field and click **Test.** The result will appear in the **Result** field.

- ***For a matching rule,*** the result will be "matched" or "not matched," or if an exclusion is triggered, "exclusion matched."
- ***For a rewriting rule,*** the result will be the rewritten expression.


Header Rewrite Rule Wizard -- Webpage Dialog

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/headerrewriterulewizard.asp

Rule Completion

Test Rule

To test the rule, enter a sample string in the Source field and click Test. If the result is not as expected, click Back to return to other windows of the wizard.

Source: joe@internalserver.example.com <joe@internalserver.example.com>

Result: joe@example.com <joe@example.com>

Test
Back
[100%]
Help
Finish
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/heade
Internet

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.*

CONFIGURING REPUTATION SERVICES

MailMarshal SPE can retrieve information from DNS based blacklists or Reputation Services such as SpamCop and SpamHaus.

Configuring a DNS Blacklist for use in MailMarshal SPE is a two step process. You configure details of the list in Array configuration, then you configure one or more receiver rules to filter email based on the list information

For more information, see “Reputation Services” on page 99.

Chapter 7
Understanding Email Policy, Policy Groups, and Rules

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

The Email Policy consists of Array Policy, Customer Packages, and Advanced Customer Defined policies. Each of these parts can contain Incoming and Outgoing policy groups. A policy group contains one or more rules.

Understanding Policies and Policy Groups

A **policy group** is a group of rules that controls email processing in MailMarshal SPE. A **policy** is a set of policy groups.

MailMarshal SPE includes three types of policy to provide email content security management for multiple customers:

Array Policy

These policies are applied to all messages passing through a specific array of MailMarshal SMTP Servers.

Customer Packages

These policies are applied for one or more customer organizations. You can choose to apply the policies by default for new customers. You can set additional options for each policy in a package. For instance, you can hide a policy from customers, or allow customers to make exceptions to it.

Advanced (Customer defined)

These policies are defined by Customer Administrators through the Customer Web Console (available to Advanced customers only). The policies are specific to the individual customer organizations.

Note: *Most, but not all, of the Rule Conditions and Rule Actions listed in this Guide are available to Advanced Customers. Advanced customers also have access to a limited "Pass to Rule" action that is not available to Service Providers. For full details of the items available to customers, see the User Guide.*

This structure allows you to apply policies in a granular manner. Policies can apply to all arrays and customers, or to certain arrays only, or to certain customers only.

You can choose to use just a few policy groups, or many. For example, you could use one Outgoing policy group to contain rules that apply to all messages outbound from the Service Provider, and three Incoming policy groups to contain rules that apply to three different types of customer subscriptions. You can also use policy groups to manage hardware resources and allocate tasks such as virus scanning to arrays of MailMarshal SMTP Servers.

Policies and Rules are evaluated by the MailMarshal SMTP servers that process messages. For more details about how Rules are applied, see "Understanding Rules" on page 167 and "Understanding the Order of Evaluation" on page 204.

You can view and print a summary of a selected Array Policy or Customer Package. See "Displaying Policy Summaries" on page 206.

Creating Policies and Policy Groups

To review, create, or edit a policy:

1. In the left pane of the Administration Console, select Array Policy or Customer Packages.
2. ***If you want to create a new Policy,*** on the main window click **New.**
3. ***If you want to duplicate an existing Policy,*** on the main window select the group and then click **Duplicate.**
4. ***If you want to edit an existing Policy,*** on the main window select the group and then click **Edit**.
5. On the Policy window, specify the following information:
   a. Enter the policy name and description to identify the Policy.
   b. Optionally choose to select the policy by default for new arrays. For Array Policies, when editing you can also choose not to enforce use of configured domains. For more information about these settings, see Help.
   c. Select the arrays or the customers this policy will apply to.
6. Click **OK** to save changes.

If you have more than one Array or Customer policy, you can choose the order in which MailMarshal SPE processes them. See “Understanding the Order of Evaluation” on page 204.

You can enable or disable a policy to quickly modify configuration. To enable or disable a policy, on the main window select the policy and then click **Enable** or **Disable.**

To review, create, or edit a policy group:

1. In the left pane of the Administration Console, expand Array Policy or Customer Packages, and select the parent policy.
2. ***If you want to create a new Group,*** on the main window click **New.**
3. ***If you want to duplicate an existing Group,*** on the main window select the group and then click **Duplicate.**
4. ***If you want to edit an existing Group,*** on the main window select the group and then click **Edit**.
5. On the Policy Group window, enter the group name and description
6. Choose to apply the Group to Inbound or Outbound messages.
   - Inbound Policy matches if the message is addressed to a domain that is included in the Domains list for the customer.
   - Outbound policy matches if the message is addressed to a domain that is not included in the Domains list for the customer
7. Select additional options.
8. Click **OK** to save changes.

Additional Policy Group Options

You can choose how Policy Groups apply to customers, and how much control customers have over the Policy Groups.

- You can **hide** a Policy Group from customers completely. The rules will apply to messages but will not be visible in the Customer Console. Rule actions may still be visible in reports and message history.
- You can allow customers to **disable** a Policy Group.
- You can allow customers to make **exceptions** to a Policy Group, for particular User Groups.

Policy groups have three states: Enabled, Disabled, and Deactivated.

- **Enabled groups** are available to customers. When a customer is given access to an enabled group, by default the group will be used for email processing. You can choose to allow customers to disable a group.
- **Disabled groups** are available to customers. When a customer is given access to a disabled group, by default the group *will not* be used for email processing. You can choose to allow customers to enable a group.
- **Deactivated groups** are not available for selection by customers. If you deactivate a group it will be deactivated for any customers currently using it.

You can enable, disable, or deactivate a policy group to quickly modify configuration. To enable, disable, or deactivate a group, on the main window select the group and then click the appropriate button.

Note: *If a customer has access to a group, selecting enabled or disabled status for that group does not change the enabled/disabled state of the group for the customer.*

For more information about setting policy group options, see Help.

UNDERSTANDING RULES

MailMarshal 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 applies receiver rules while the MailMarshal Receiver is receiving a message from a remote email server. A receiver rule can cause MailMarshal 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 applies standard rules after a message has been fully received. They are processed by the MailMarshal 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.

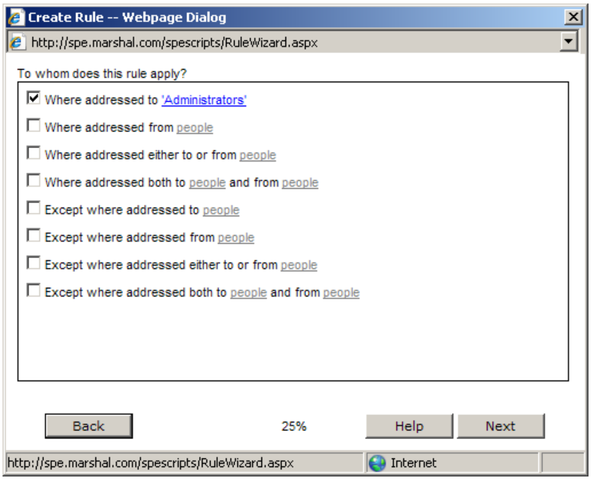
Creating Rules

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 Administration Web Console, select a policy group.
2. In the main pane, click **New**.
3. On the first window of the rule wizard, choose to create a receiver rule or a standard rule.

4. In the User Matching window, select the User Matching conditions for this rule.



Create Rule -- Webpage Dialog
http://spe.marshal.com/spescripts/RuleWizard.aspx

To whom does this rule apply?

☑ Where addressed to 'Administrators'
□ Where addressed from people
□ Where addressed either to or from people
□ Where addressed both to people and from people
□ Except where addressed to people
□ Except where addressed from people
□ Except where addressed either to or from people
□ Except where addressed both to people and from people

Back
25%
Help
Next
http://spe.marshal.com/spescripts/RuleWizard.aspx
Internet

5. If you must enter more information to define a condition, the description of the condition includes a hyperlink. Click the hyperlink of a selected item to open a rule condition window that allows you to enter the required information.

6. To continue to the Rule Conditions window, click **Next**.

7. In the Rule Conditions window, select the conditions for this rule. Specify any additional information required as for Step **5**.

8. To continue to the Rule Actions window, click **Next**.

9. In the Rule Actions window, select the actions for this rule. Specify any additional information required as for Step **5**.

10. On the Rule Completion window, review the rule description. Enter a name and optional comment or explanation of this rule.

  a. For Array Policies, choose whether the rule is enabled or disabled using the **Enable Rule** box

  b. For Package Policies, choose the default state of the rule using the **Rule State** menu, and choose what options are available to customers using the additional checkboxes.

To create the rule and complete the wizard, click **Finish**.

Making Copies Of Rules

You can create a copy of a rule in the same policy group, or in another policy group.

- ***If you want to make a copy in the same group,*** while viewing a group select a rule, and then click **Duplicate**.
- ***If you want to make a copy in another group,*** while viewing a group select a rule, and then click **Copy**.

Note: *If you copy a rule from an Inbound to an Outbound policy (or vice versa), MailMarshal SPE rewrites the user matching section of the rule so that the “from” and “to” sections apply to appropriate addresses. If the rule uses a folder, MailMarshal SPE also changes the folder from the “incoming” to the “outgoing” folder (or vice versa). You should check the copied rule carefully before using it in production.*

UNDERSTANDING USER MATCHING

MailMarshal 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 in MailMarshal SPE are based on user groups. User groups can include wildcard entries.

Note: *In MailMarshal SPE installations, the Policy types (array, customer package, or customer defined) override User Matching. If a policy is not used by an array, or is not applied to a specific customer, then user matching is not relevant.*

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

The available User Matching conditions include the following:

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”, you can select one or more User Groups. For more information about User Groups, see “Configuring User Groups” on page 116.*

Where addressed from people

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

Where addressed either to or from people

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

Where addressed both to people and from people

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

Except where addressed to people

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

Except where addressed from people

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

Except where addressed either to or from people

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

Except where addressed both to people and from people

Requires two lists of groups. Matches if the sender of the message is **not** found in the first list of groups specified, and **no** recipient of the message is found in the second list of groups specified.

***Tip:** "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 addressed to Chicago Staff except where addressed to Managers.`

UNDERSTANDING RULE CONDITIONS

MailMarshal SPE uses the MailMarshal SMTP infrastructure to evaluate rule conditions within standard and receiver rules. MailMarshal checks rule conditions after any User Matching conditions. In general MailMarshal 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. If the condition includes options, arguments, or variables, you can click a hyperlink in the rule wizard to open a rule condition window and specify values.

Note: *This section lists all rule conditions. Some conditions may not be available to you because MailMarshal SPE licensing options affect which conditions are available.*

- *Anti-Virus: Includes only a few conditions required to apply virus scanning.*
- *Anti-Spam: Includes a number of items related to spam identification, including IP range, TextCensor, safe senders, and Category Script conditions.*
- *SpamProfiler: Includes the Receiver and Rule conditions for SpamProfiler*
- *Content Scanning: Includes nearly all conditions.*

For exact details of the conditions available under each option, see M86 Knowledge Base article Q12167.

Rule Conditions for Standard Rules

The following conditions are available for use in standard rules in MailMarshal SPE. 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 sender’s IP address matches address
- Where the result of Blended Threat Module analysis is
- Where message attachment is of type
- 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 message triggers System Text Censor script(s)
- Where the external command is triggered *(Only available in Array Policy)*

- Where attachment parent type is
- 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 the sender is/is not in the recipient's safe senders list
- Where message is categorized as category
- Where message spoofing analysis is based on criteria
- Where the attached image is/is not/may be inappropriate

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 (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.

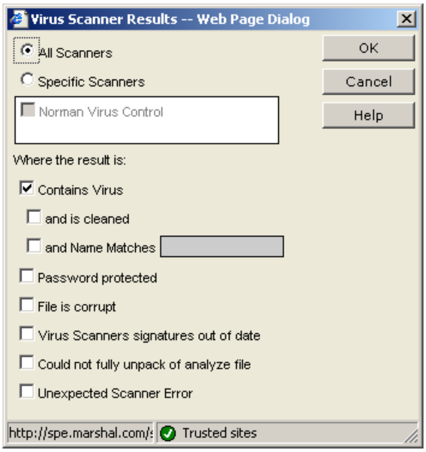
Note: *You can also choose to reject messages at the Receiver based on SpamProfiler evaluation. For more information, see "Spam" on page 89.*

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

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. Use the rule condition window to choose the desired virus scanning action and the results to be checked for.



Virus Scanner Results -- Web Page Dialog

● All Scanners

○ Specific Scanners

□ Norman Virus Control

Where the result is:

☑ Contains Virus

□ and is cleaned

□ and Name Matches

□ Password protected

□ File is corrupt

□ Virus Scanners signatures out of date

□ Could not fully unpack of analyze file

□ Unexpected Scanner Error

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

Note: *If the MailMarshal SPE installation includes more than one Array, the same virus scanners most be installed on all email processing servers of all arrays. You must install the scanner software on each server and add the scanners using the MailMarshal Configurator on each Array Manager.*

Use integrated DLL based scanners for production. Use of Command Line scanners is not supported by M86 Security.

- **All Scanners:** MailMarshal uses all configured virus scanners to scan all parts of the message and attachments.
- **Specific scanners:** To limit the virus scan to specific installed scanners, choose this option then select the desired scanners from the list. MailMarshal 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 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 233.
- **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 will not allow you to save your selections.*

Use the option “Unexpected scanner error” to specify an action MailMarshal should take when the code returned by the scanner is not known to MailMarshal. If this option is not selected in a rule condition, an unexpected return code will result in the message being dead lettered.

To Set Up Virus Cleaning

If you want MailMarshal to attempt to “clean” viruses from email messages, you must install at least one DLL based virus scanner and set up two 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 takes the following actions:

1. MailMarshal 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 deadletters the affected message.
3. The message log and MailMarshal Engine log will indicate that the message still contains a virus.
4. If you choose to forward or process the affected message, MailMarshal displays a warning indicating that the message contains a virus.

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, use this condition in a receiver rule where possible.*

MailMarshal shows the configured ranges in the rule condition window. To add a range to the list, click **New** then enter the required data. To modify an existing address, highlight it then click **Edit.** To delete an existing address from the list, highlight it then click **Delete**.

Add or modify an address or range by entering data in the fields You can enter any of the following:

- **A single 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) in the **IP Address** and **To** columns. 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 in the **IP Address** and **Network Mask** columns. For instance, enter “10.2.1.4” and “255.255.255.0” to match the entire 10.2.1.0 subnet.

The check box **Excluded** 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 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 M86 Security 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. For details of the options available with this condition, see Help

Notes: *If the Blended Threats Module is not licensed, it is not available for selection.*

- *If the Blended Threats Module license expires while this condition is selected, MailMarshal SPE removes this rule condition from the configuration sent to MailMarshal SMTP arrays.*
- *For more information about the Blended Threats Module, see M86 Knowledge Base article* Q12876*.*

Where message attachment is of type

MailMarshal checks the structure of all attached files to determine their type. MailMarshal 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 add custom file types. See “Configuring Custom File Types” on page 109.*

Where message size is

MailMarshal 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 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 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;*.DO?`

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. For information about adding and editing Scripts, see “Identifying Email Text Content Using TextCensor Scripts” on page 120.

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 message triggers System Text Censor script(s)

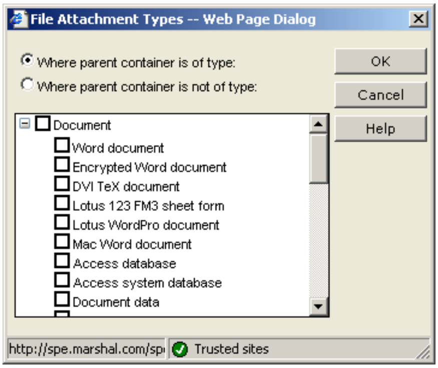
This condition checks textual content using System TextCensor Scripts. For detailed information about Scripts, see “Identifying Email Text Content Using TextCensor Scripts” on page 120

Where the external command is triggered

This option allows you to select one or more external commands MailMarshal 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 “Configuring External Commands” on page 107.

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 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 Microsoft Word document.



File Attachment Types -- Web Page Dialog

● Where parent container is of type:
○ Where parent container is not of type:

- □ Document
  - □ Word document
  - □ Encrypted Word document
  - □ DVI TeX document
  - □ Lotus 123 FM3 sheet form
  - □ Lotus WordPro document
  - □ Mac Word document
  - □ Access database
  - □ Access system database
  - □ Document data

http://spe.marshal.com/sp Trusted sites

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.

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 155.

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 then click **Edit** to restart the Header Matching Wizard. To delete a Header Match condition, highlight it 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 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 message recipient through the optional Spam Quarantine Management (SQM) web function. A typical use of this action is to create an exception to Spam and Junk Mail rules, using the rule action "Pass the message to rule.".

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

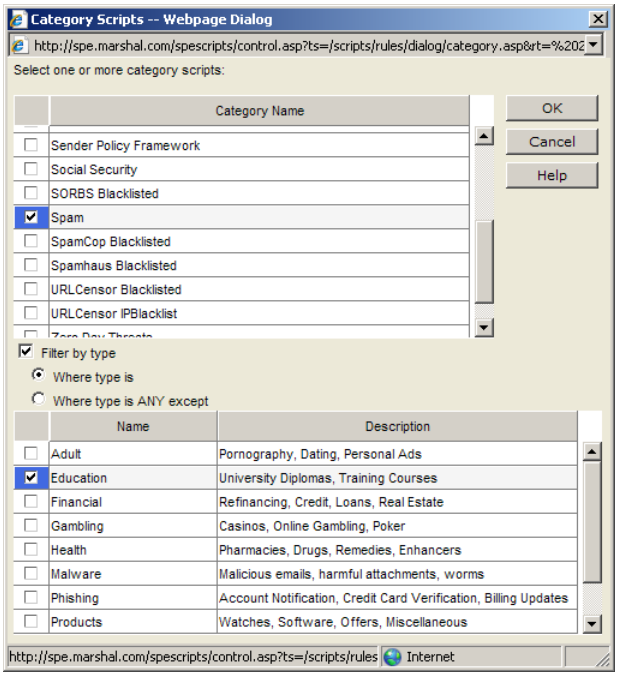
In the rule condition window, choose whether to apply the condition if the sender is, or is not, in the recipient’s safe senders list.

Note: *If SQM is not enabled for a customer, or if the Safe Senders list is disabled (from the SQM Administrator page), this condition has no effect.*

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.


Category Scripts -- Webpage Dialog
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/category.asp&rt=%202
OK
Cancel
Help
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules
Internet

Select one or more category scripts:

	Category Name
□	Sender Policy Framework
□	Social Security
□	SORBS Blacklisted
☑	Spam
□	SpamCop Blacklisted
□	Spamhaus Blacklisted
□	URLCensor Blacklisted
□	URLCensor IPBlacklist
□	Zero Day Threats

☑ Filter by type

● Where type is

○ Where type is ANY except

	Name	Description
□	Adult	Pornography, Dating, Personal Ads
☑	Education	University Diplomas, Training Courses
□	Financial	Refinancing, Credit, Loans, Real Estate
□	Gambling	Casinos, Online Gambling, Poker
□	Health	Pharmacies, Drugs, Remedies, Enhancers
□	Malware	Malicious emails, harmful attachments, worms
□	Phishing	Account Notification, Credit Card Verification, Billing Updates
□	Products	Watches, Software, Offers, Miscellaneous

***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 can automatically download updates to category scripts. The MailMarshal SpamCensor is an automatically updated category script.

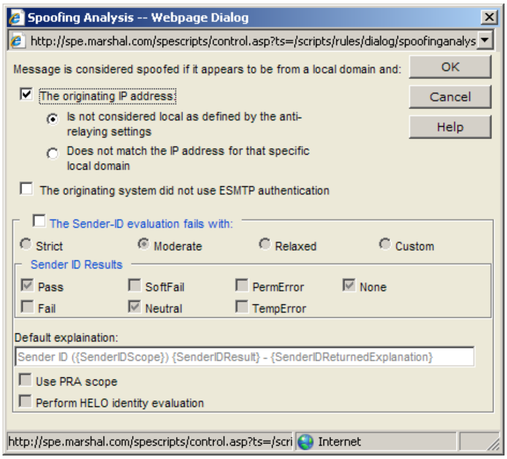
You can create and customize your own category scripts. Some example category scripts are provided with MailMarshal. For more information, see the white paper “MailMarshal SMTP for Anti-Spam,” available from the MailMarshal SMTP support page on the M86 website.

Where message spoofing analysis is based on criteria

This condition allows you to define when MailMarshal 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.



Spoofing Analysis -- Webpage Dialog

http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/spoofinganalys

Message is considered spoofed if it appears to be from a local domain and:

☑ The originating IP address:

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

○ Does not match the IP address for that specific local domain

□ The originating system did not use ESMTP authentication

□ The Sender-ID evaluation fails with:

○ Strict ● Moderate ○ Relaxed ○ Custom

Sender ID Results

☑ Pass □ SoftFail □ PermError ☑ None

□ Fail ☑ Neutral □ TempError

Default explaination:

Sender ID ({SenderIDScope}) {SenderIDResult} - {SenderIDReturnedExplanation}

□ Use PRA scope

□ Perform HELO identity evaluation

http://spe.marshal.com/spescripts/control.asp?ts=/scri Internet

MailMarshal 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 by the domains associated with customers allocated to this array. 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 checks the IP address:

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

When you select this option, MailMarshal 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 entered on the Relaying Sources tab of Server and Array Properties.

This option is useful if you allow multiple servers to route email directly through MailMarshal.

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

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

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

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. See Help for detailed information about the Sender ID criteria.

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

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

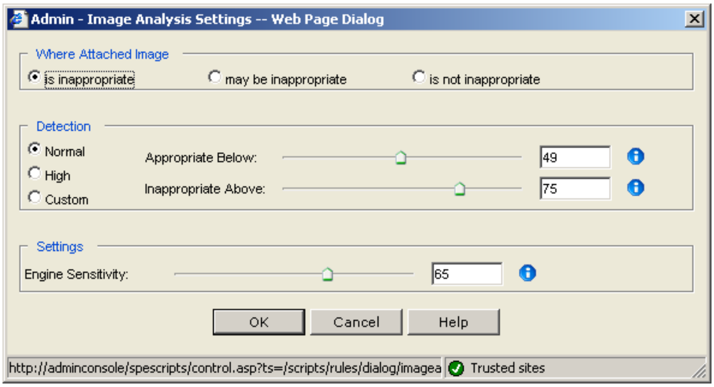
This condition allows you to take action on a message based on the result of analysis of attached images by Image Analyzer (an optional component licensed separately).

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.



Admin - Image Analysis Settings -- Web Page Dialog

Where Attached Image

● is inappropriate ○ may be inappropriate ○ is not inappropriate

Detection

● Normal
○ High
○ Custom

Appropriate Below: 49

Inappropriate Above: 75

Settings

Engine Sensitivity: 65

http://adminconsole/spescripts/control.asp?ts=/scripts/rules/dialog/imagea Trusted sites

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.

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 controls 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 the following 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.

Rule Conditions for Receiver Rules

The following conditions are available for use in receiver rules.

- Where sender has authenticated
- Where sender's IP address is listed by Reputation Service
- Where message size is
- Where sender’s IP address matches address

- Where sender's HELO name is/is not
- Where the SPF evaluation result is

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 authenticated the remote system using an account and password. For more information about setting up accounts for authentication see “Configuring Accounts” on page 106. You may need to create an Array Authentication rule for this condition to work reliably. See the Receiver section in “Advanced Options for Array Properties” on page 92.

Where sender's IP address is listed by Reputation Service

This condition allows Reputation Service (DNS Blacklist) tests 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 Services you want to use. Clear the check box for any Services you do not want to use in this Condition. For information about configuring services, see “Reputation Services” on page 99.

Where message size is

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 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 shows the configured ranges in the rule condition window. To add a range to the list, click **New** then enter the required data. To modify an existing address, highlight it then click **Edit.** To delete an existing address from the list, highlight it then click **Delete**.

Add or modify an address or range by entering data in the fields You can enter any of the following:

- **A single 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) in the **IP Address** and **To** columns. 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 in the **IP Address** and **Network Mask** columns. For instance, enter “10.2.1.4” and “255.255.255.0” to match the entire 10.2.1.0 subnet.

The check box **Excluded** 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's HELO name is/is not criteria

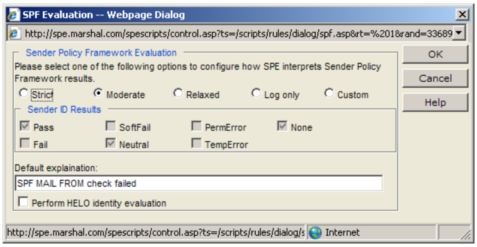
This condition allows action to be taken based on the HELO name provided by the remote email server. Choose from the following options:

- **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).
  - **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.

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

Where the SPF evaluation result is

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


SPF Evaluation -- Webpage Dialog
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/spf.asp&rt=%201&rand=33689
OK
Cancel
Help
http://spe.marshal.com/spescripts/control.asp?ts=/scripts/rules/dialog/s
Internet

Sender Policy Framework Evaluation

Please select one of the following options to configure how SPE interprets Sender Policy Framework results.

○ Strict ● Moderate ○ Relaxed ○ Log only ○ Custom

Sender ID Results

☑ Pass ☐ SoftFail ☐ PermError ☑ None
☐ Fail ☑ Neutral ☐ TempError

Default explaination:
SPF MAIL FROM check failed

☐ Perform HELO identity evaluation

To select a custom triggering value, and to configure advanced options, select Custom and then edit the settings.

See Help for definitions of the options.

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

UNDERSTANDING RULE ACTIONS

MailMarshal rule actions are performed by standard and receiver rules. MailMarshal 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 rule. MailMarshal 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 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 test following.

- Copy the message to folder with release action
- BCC a copy of the message
- Run the external command (Only available in Array Policy)
- Send an E-mail Notification message
- Strip attachments
- Write log message with classification *(Mandatory for terminal actions and copy to folder)*
- Stamp message with message stamp
- Rewrite message headers
- Set message routing to host
- Move the message to folder with release action *(terminal action)*
- Park the message for later delivery in folder *(terminal action)*
- Delete the message *(terminal action)*
- Pass message on to rule

Copy the message to folder with release action

This action copies the email message file to the specified archive folder. You must also specify a release action. If the message is released (through the Console, SQM, or Message Release command), processing resumes according to the selection you make. You can choose to resume from the next rule, the next policy group, or a specific rule. You must include a classification action to ensure that the message can be searched for and acted on.

Notes: *The release action has the following limitations:*

- *You can select the “skip to specific rule” option when editing, but not when adding a new rule.*
- *You can only skip to a rule in the current policy group that is enabled and evaluated after the current rule.*
- *You cannot move the target rule of a “skip to” condition above the rule that performs the “skip to.” You cannot disable or delete the target rule.*

For more information about folders in MailMarshal SPE, see “Using Email Folders” on page 151.

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. 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 SPE.

Choose one or more commands to be run from the list of pre-defined external commands. For information about defining external commands, see “Configuring External Commands” on page 107. To run the same application with different parameters under different conditions, use more than one external command definition.

Send an Email notification message

This action sends one or more email messages based on the templates selected in the rule action window. For further information about templates, see “Notifying Users with Message Templates” on page 130.

Strip Attachments

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.

Note: *MailMarshal 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.*

Write log Message with classification

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

All rules that include a terminal action (move, park, or delete) must include a classification action. This requirement allows accurate administration and reporting on messages blocked by MailMarshal SPE.

Select a single logging classification from the list in the rule action window. For details on classifications, see “Using Message Classifications and Classification Groups” on page 111.

Tip: *In MailMarshal SPE, classifications control message viewing, pass through, and other options. You can only select one classification for a message.*

Stamp message with message stamp

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. For details on adding and editing message stamps, see “Notifying Users with Message Stamps” on page 141.

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, shown below, 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 156.

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.*

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.

MailMarshal uses this address when it attempts delivery, even if the message is “parked” first. If several rules invoke this action, MailMarshal uses the last address.

Note: *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 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.*

Move the Message to folder with release action

This action moves the email message file to the specified quarantine folder. You must also specify a release action. If the message is released (through the Console, SQM, or Message Release command), processing resumes according to the selection you make. You can choose to resume from the next rule, the next policy group, or a specific rule.

Notes: *The release action has the following limitations:*

- *You can select the "skip to specific rule" option when editing, but not when adding a new rule.*
- *You can only skip to a rule in the current policy group that is enabled and evaluated after the current rule.*
- *You cannot move the target rule of a "skip to" condition above the rule that performs the "skip to." You cannot disable or delete the target rule.*

This is a terminal action. MailMarshal does not process any further rules for a message if this action is performed, unless the message is later released. Any rule that includes this action must also include a log classification.

Park the Message for Later Delivery in folder

This action moves the email message file to the specified parking folder for release according to the schedule associated with that folder.

This is a terminal action. If this action is performed, MailMarshal does not process any further rules for a message until the message is released from the parking folder. Any rule that includes this action must also include a log classification.

Delete the Message

This action deletes the email message file. The message will not be sent to its original destination.

This is a terminal action. MailMarshal does not process any further rules for a message if this action is performed. Any rule that includes this action must also include a log classification.

You can choose to delete the message without creating a MailMarshal log record. This option is intended for use when the message will be forwarded to another server for processing and returned to MailMarshal (for instance, when using MailMarshal SES for encryption). *Use this option with extreme caution as it can make messages completely untraceable.*

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 rule.

Notes: *This action has the following limitations:*

- *You can select the “skip to specific rule” option when editing, but not when adding a new rule.*
- *You can only skip to a rule in the current policy group that is enabled and evaluated after the current rule.*
- *You cannot move the target rule of a “skip to” condition above the rule that performs the “skip to.” You cannot disable or delete the target rule.*

Rule Actions for Receiver Rules

The following actions are available for use in receiver rules.

- Refuse message and reply with message

- Accept message
- Continue processing rules

Note: *These actions take effect immediately. If you use both “accept” and “refuse” actions in receiver rules, check the order of evaluation carefully to ensure that MailMarshal checks for any exceptions first.*

Refuse message and reply with message

This action directs MailMarshal to refuse the message. MailMarshal 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 DNS Blacklist 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.

Accept message

This action directs MailMarshal to accept the message for delivery subject to standard rules. The message could be relayed to an address outside the 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.

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.”

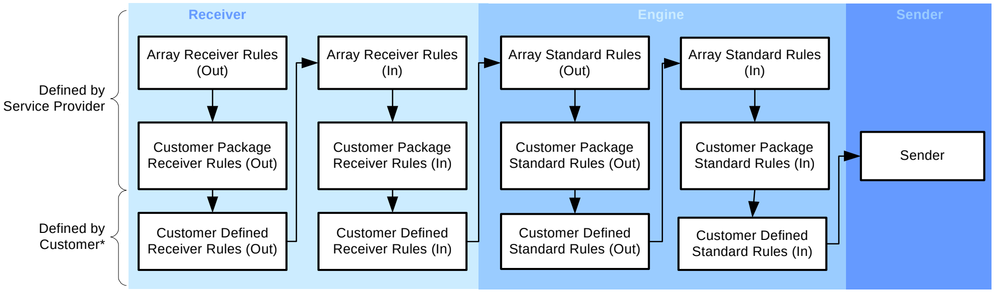
UNDERSTANDING THE ORDER OF EVALUATION

The order in which MailMarshal SPE evaluates policy groups and rules can affect the outcome of processing for a message. This can be due to the layers of policy present, and also can be due to “terminal” actions that stop MailMarshal processing further rules for a given message.

For instance, dangerous file type rules are normally evaluated before virus scanning rules. If a file type is not permitted, MailMarshal SPE quarantines the message immediately, without using processing time on the virus scan.

Note: *If the message is later released, remaining rules will be processed and the virus scan will be performed at that time.*

MailMarshal SPE evaluates receiver rules before standard rules. Within each type of rules, MailMarshal evaluates Outbound rules first, then Inbound rules. MailMarshal evaluates global rules first, then Service Provider defined rules, and finally customer defined rules if any. The order of evaluation for rule types is summarized in the following chart.


Receiver
Engine
Sender
Defined by Service Provider
Defined by Customer*
Array Receiver Rules (Out)
Customer Package Receiver Rules (Out)
Customer Defined Receiver Rules (Out)
Array Receiver Rules (In)
Customer Package Receiver Rules (In)
Customer Defined Receiver Rules (In)
Array Standard Rules (Out)
Customer Package Standard Rules (Out)
Customer Defined Standard Rules (Out)
Array Standard Rules (In)
Customer Package Standard Rules (In)
Customer Defined Standard Rules (In)
Sender

* Availability of Customer Package Rules and Customer Defined Rules depends on subscription options set by the Service Provider.

Adjusting the Order of Evaluation of Policy Groups

You can change the order of evaluation for policy groups by changing the order of the policy group listing in the Web Console.

To adjust the order of evaluation of policy groups:

1. In the left pane of the Administration Web Console, expand the **Array Policy** item or the **Customer Packages** item. Select a policy.
2. Select a policy group in the right pane.
3. Move the group up or down using the buttons.
4. The change will be applied to the email processing servers at the next replication.

Note: *MailMarshal SPE always processes outbound policies before inbound policies.*

Adjusting the Order of Evaluation of Rules

You can change the order of evaluation of rules within a Policy Group by changing the order of the rule listing in the Administration console.

To adjust the order of evaluation of rules:

1. In the left pane of the Administration Console, expand the **Array Policy Group** item or the **Customer Packages** item. Expand a policy.
2. Select a policy group.
3. Select a rule in the main pane.
4. Move the rule up or down using the buttons.
5. The change will be applied to the email processing servers at the next replication.

Note: *Within a policy group, MailMarshal SPE lists all receiver rules first. MailMarshal SPE processes receiver rules before it accepts the body of a message, so it always applies receiver rules before standard rules.*

Displaying Policy Summaries

You can view and print a summary of a selected Array Policy or Customer Package. These summaries may be useful for internal documentation or for presentation to Customers.

To view a summary:

1. From the left pane menu, select Array Policy or Customer Packages.
2. On the right pane, select the Policy or Package you wish to view, and then click Policy Summary or Package Summary.

Chapter 8
Delegating Spam and Quarantine Management

In some cases when MailMarshal quarantines an email message as suspicious, the recipient or sender wants the message to be released to its destination. This situation is likely to arise with messages that MailMarshal has classified as spam.

MailMarshal SPE provides several options that allow the administrator to delegate the responsibility for reviewing these messages and taking action:

- Customers can delegate permission to process the messages in selected quarantine folders, using the MailMarshal SPE Customer Web Console.
- Each email user can receive a daily summary of their incoming messages that have been quarantined, through MailMarshal SPE digest emails.
- Each email user can have permission to review and release messages quarantined in one or more folders, through the MailMarshal SPE Spam Quarantine Management Website (installed with the Cusotmer WEb Console server). 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 a personal list of safe 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 SPE Message Release external command. For more information, see “Using the Message Release External Command” on page 214.
- You can control the behavior of MailMarshal when a message is released by a user. You can choose to pass the message through, or to continue processing rules. Configure this setting for folders when you add or edit a customer. For more information about adding and editing customers, see “Configuring Customers” on page 75.

SETTING UP SPAM QUARANTINE MANAGEMENT FEATURES

The MailMarshal SPE 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 SPE rules to help determine whether email sent to that user is spam.

The SQM website is hosted as a subdirectory of the Customer Web Console.

You can provide the SQM website interface in branded themes for each customer and in multiple languages. To learn more about themes in the SQM, see M86 Knowledge Base article Q12237.

Note: *The SQM function requires the Spam sub-license of MailMarshal SPE.*

Spam Quarantine Management Windows

The Spam Quarantine Management Website includes the following windows:

Log In

Allows a user to enter an email address and password to log in to the Spam Quarantine Management Website. You can choose to allow users to self-register, or you can require that all user registrations be imported by the customer administrator through the MailMarshal SPE Web Console.

Home

Allows a user to view a list of email blocked since their last visit, and optionally displays summary charts of blocked and good email.

Blocked Mail

Allows a user to review a list of email quarantined in one or more classifications. The user can view, release or delete each message. The user can also add the sender address to the safe senders list (if allowed by the administrative settings). If more than one classification is available through this site, the window 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 safe senders.

Manage Senders

Allows a user to add, edit, or delete entries in a list of safe email addresses. MailMarshal SPE uses these lists in the rule condition “Where sender is/is not in recipient’s safe senders list.”

User Settings

Allows a user to configure site and address options:

- Set the site look and feel, including language and time zone.
- Add or delete entries in a list of email addresses that they can manage using this login. Before adding a requested address to the list, MailMarshal SPE 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 safe senders lists. The delegates can choose which user’s email to review using a list at the top of the window. Delegation is an optional feature.

Change Password

Allows a user to change the password associated with their login (email address) for this site.

Help

Each window includes a link to a Help window that provides additional information about fields and functions.

To enable the Spam Quarantine Management Website:

1. In the Web Console, expand **Global Configuration > System Settings**. Select the SQM tab.
2. Select **Enable SQM**. Select a default theme, and select the options you want to be able to offer to customers. For descriptions of the options, see Help.

Note: *The setting for the SQM URL on this window only controls the URL string used in email notifications and templates. To change the web location, edit the virtual directory in IIS.*

3. Click **OK** to save the settings.

To enable SQM for a customer:

1. In the Web Console, expand **Client Configuration > Customers**.
2. Select a customer, and click **Edit**. Select the SQM tab.
3. Select **Enable SQM**. Select a default theme for the customer, and select the options the customer can use. For descriptions of the options, see Help.
4. In the Web Console, expand **Client Configuration > Domains**.
5. Edit an existing domain that is associated with the customer. On the General tab, select **Enable SQM**, and select the options for this domain. For descriptions of the options, see Help.
6. Click **OK** to save the settings.

You should define suitable customer package rules with quarantine and classification actions to make messages available in the SQM. You can specify classifications that will be available in the SQM by default, using the properties of each classification. Each customer can use the customer web console to select classifications that will display in the SQM and to define the logins that can access the SQM. If self provisioning is enabled for a customer, any user that can access the website can create a SQM login.

Note: *The SQM website uses login by email address and password. SQM logins can only be created for email addresses within the customer domain(s) that have SQM enabled.*

Setting Up Message Digests

MailMarshal allows you to send email summaries to users, notifying them about messages MailMarshal has quarantined. Users can review basic information and release the messages directly from the digest email. When SQM is in use, users can visit the SQM pages for additional options.

Digests can be created by the Service Provider, or by a customer.

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.
- Send digest emails to each user with undigested email in the folder, or send all digest emails to a specified address.

For more information about digests, see “Setting Up Message Digests” on page 138.

Setting Up Rules

MailMarshal SPE places email in quarantine classifications through rule action.

To set up spam Quarantine rules:

1. Create MailMarshal SPE rules to classify spam messages with distinct classifications.
2. Within the rule or rules, use the condition “Where the sender is in the recipient’s safe senders list.” Configure the rule so that messages that meet this condition are not classified as spam.

Note: *The user safe list condition uses the Safe Senders list maintained within the Spam Quarantine Management website. If the SQM website is not in use, or if you choose to disable these lists (globally or per customer), then these rule conditions will have no effect.*

3. When a user releases a message, MailMarshal SPE can forward the message to its destination without further processing or can continue processing the message, beginning with the rule that follows immediately after the rule that quarantined the message. To configure this option for customer folders, use the Folder Settings tab of the Customer properties. To configure this option for array folders, use the properties of the specific folder.

Setting Up Spam Quarantine Management for Other Classifications

Each customer can configure any message classification to be managed through the Spam Quarantine Management Website. This function is available in the **SQM Classifications** item of the Customer Web Console. The release action for a message depends on the action for the folder where the message is quarantined.

USING THE MESSAGE RELEASE EXTERNAL COMMAND

Some MailMarshal SPE 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 provides a message release function for these situations. Message Releasing allows MailMarshal 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.

Automatic Message Release should be used sparingly as it tends to defeat the purpose of email filtering.

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}. 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* ***the same MailMarshal array that generated the notification.*** *The address need not be valid but it must be well-formed.*

To process message release requests, create a MailMarshal SPE 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. The {ReleaseProcessRemaining} variable is more secure because it forces all messages to be evaluated against all rules.

When a managed MailMarshal SMTP installation is configured as an array with separate Array Manager and processing servers, the Message Release command must provide a Windows credential that the Array Manager can validate. 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] [-l] {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 is generally required where a MailMarshal SMTP array has multiple processing servers.

Note: *You must include the password value.*

`-l` 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 9
MailMarshal SPE Monitoring, Auditing, and Reporting

MailMarshal SPE provides a number of views to assist in daily administration of email flow and server health. These include the Reports, Scheduled Reports, Agent Status Page, Rule Summaries, Audit History, Windows event logs, and the text logs generated by each MailMarshal SPE Agent service.

If you want to:	Use:
View a summary of email traffic and filtering activity for the current day; view details of configuration update status and statistics on all running MailMarshal SMTP Array Managers	The MailMarshal Today page in the Administration Console. See “Understanding The MailMarshal Today Page” on page 65.
View details of messages queued for sending to external domains; delete a message queued for sending to an external domain	The Array Status page in the Administration Console. See “Monitoring Array and Server Status” on page 229.
View totals of messages processed and queued for each email processing server; view details of messages processed for customers; delete a message queued for sending to a customer domain	The Message Queues, Reports and Mail History in the Administrator or Customer Web Console. See the *User Guide* for details of reports. You can log in to the Customer Web Console using the default SPE Support login. For details, see “Administrative Logins” on page 56.
View a history of status messages for all MailMarshal SPE Agent services	The Agents Status in the Administration Console. See “Monitoring Agent Services” on page 228.

If you want to:	Use:
View a history of status messages for all MailMarshal SMTP Array Managers and servers	The Array and Server Status in the Administration Console. See “Monitoring Array and Server Status” on page 229.
Stop and start MailMarshal SPE Agent services	The Windows Services control panel. See “Understanding Agent Services” on page 69.
Search for details of a specific message	The Mail History Search in the Administration Console. For more information, see “Using Mail History” on page 221.
View, release, redirect, or delete a message in quarantine	The History Search and folders in the Console.
View a graphical display of performance information for the MailMarshal SMTP services	The MailMarshal SPE Service Level Report, and the Windows Performance monitor. For more information, see “Available Reports” on page 225, and “Performance Monitor” on page 232.
View detailed debugging information for the MailMarshal SMTP filtering and delivery services	The Windows Application log and the MailMarshal text service logs on each server. For more information, see “Using MailMarshal SPE Logs” on page 230.
View a summary of Array Policies or Customer Packages.	The Policy Summary or Package Summary features in the Administration Console. See “Displaying Policy Summaries” on page 206.
Generate detailed reports on email traffic and filtering activity over time	MailMarshal SPE Reports. For more information, see “Generating Reports” on page 224.
Delegate administrative functions to help desk personnel	The Menu Security tab in the Admin Logins area of the Administration Console, and the Logins item in the Customer Web Console. For more information, see “Managing MailMarshal Infrastructure” on page 82 and the *User Guide*.

If you want to:	Use:
Delegate management of spam and other quarantined messages to email users	Email message templates and Digest email messages, and/or the SQM functions administered from the Customer Web Console. See “Setting Up Message Digests” on page 138 and the *User Guide* document.

VIEWING SERVER STATISTICS

The MailMarshal Today page in the Administration Console provides basic information about MailMarshal SPE infrastructure at a glance. To view the MailMarshal Today page, select MailMarshal Today in the left pane.

MailMarshal SPE collects server information for each MailMarshal SMTP Array Manager. Mail Statistics are provided for each Array Manager.

Information available on this page includes the following items:

Server Summary
Information on the MailMarshal SPE Web Console server and shows the software version as well as the configuration state of the server.

Mail Statistics for Array: array name
Shows each array’s message traffic for the current day, divided into inbound and outbound traffic. Inbound traffic is email addressed to the local domains as managed your Service Provider. Mail Statistics also shows the total number of messages currently in the MailMarshal quarantine.

Inappropriate Content (Inbound) for Array: array name
Shows the volume of each array’s inbound messages that have been classified as spam and virus infected. 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 “Working With Classification Groups” on page 114.

Inappropriate Content (Outbound) for Array: array name
Shows the volume of each array's inbound messages that have been classified as spam and virus infected. The data can include one or more folders or message classifications.

VIEWING MAILMARSHAL AUDIT TRAIL

MailMarshal SPE tracks all database events. Some of the events included are user log on, create, edit, and remove actions taken by the user, and message release/reprocess activity.

When the MailMarshal SPE SQM is in use, MailMarshal SPE tracks SQM events including administrative actions and message actions.

To view an audit trail:

1. Select Audit History in the left pane of the Administration Console.
2. On the main pane, choose the Audit Settings to narrow the search result:
   a. Select All Customers or individual organizations
   b. Select the Domain Login that belongs to the Customer
   c. Pick the action type to view. For instance, you may want to find Admin Changes to see changes made by the Service Provider Administrators.
   d. Specify a date range to perform audit history.
   e. Select how many rows of results you would like displayed per page.
   f. Select how you would like the search results sorted.
   g. Select the direction the results should be sorted in, either Ascending or Descending.

3. Click **View** to generate the Audit Trail.
4. After you generate the Audit Trail, you can save it to an XML file. To create the file, click **Download Audit Trail**.

To view an SQM audit trail:

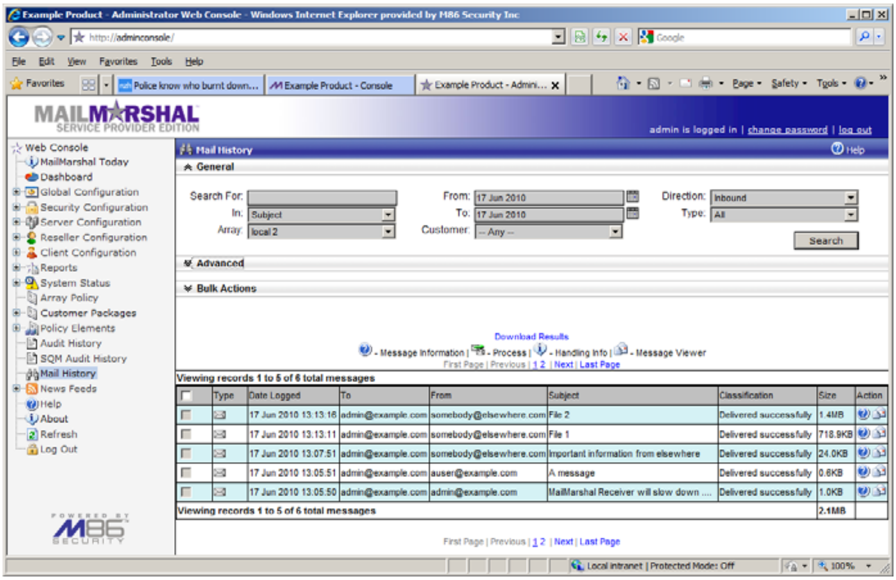
1. Select SQM Audit History in the left pane of the Administration Console.
2. On the main pane, choose the Audit Settings to narrow the search result:
   a. Select All Customers or individual organizations
   b. Select the Operator and the Target user.
   c. Pick the action type to view. For instance, you may want to find Admin Changes to see changes made by the Service Provider Administrators.
   d. Specify a date range to perform audit history.
   e. Select how many rows of results you would like displayed per page.
   f. Select how you would like the search results sorted.
   g. Select the direction the results should be sorted in, either Ascending or Descending.
3. Click **View** to generate the SQM Audit Trail.

USING MAIL HISTORY

MailMarshal SPE tracks all email messages. Mail History allows you to search for specific messages or event types for a specific customer.

To view mail history:

1. Select **Mail History** in the left pane of the Administration Console.
2. On the main pane, choose the settings to narrow the search result. Optionally expand the Advanced section to see more search criteria. For details of the fields, see **Help**.
3. Click **Search** to generate the history results. The result window lists messages that meet the criteria.



Search For:
In: Subject
Array: local 2
From: 17 Jun 2010
To: 17 Jun 2010
Customer: -- Any --
Direction: Inbound
Type: All

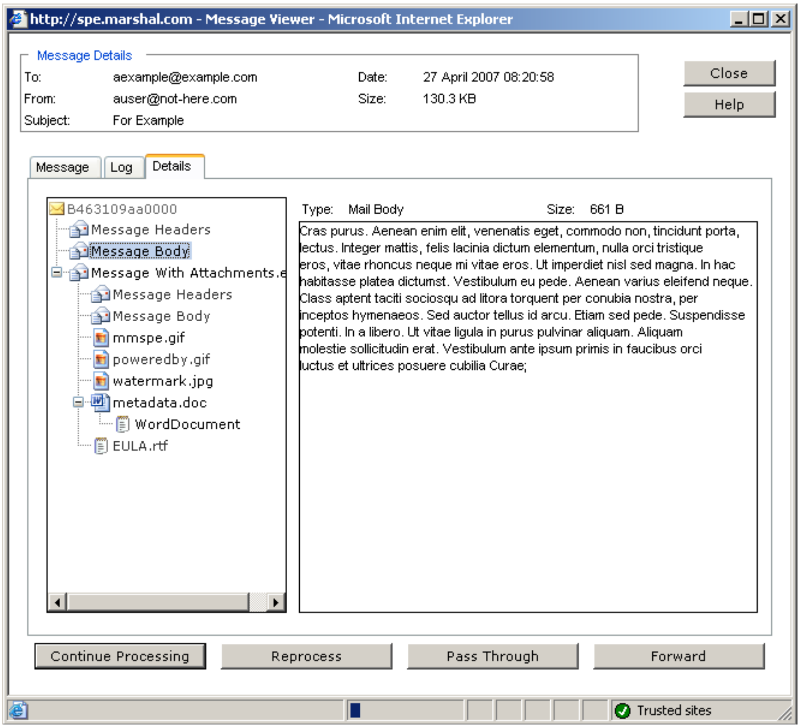
Viewing records 1 to 5 of 6 total messages

□	Type	Date Logged	To	From	Subject	Classification	Size	Action
□	✉	17 Jun 2010 13:13:16	admin@example.com	somebody@elsewhere.com	File 2	Delivered successfully	1.4MB	
□	✉	17 Jun 2010 13:13:11	admin@example.com	somebody@elsewhere.com	File 1	Delivered successfully	718.9KB	
□	✉	17 Jun 2010 13:07:51	admin@example.com	somebody@elsewhere.com	Important information from elsewhere	Delivered successfully	24.0KB	
□	✉	17 Jun 2010 13:05:51	admin@example.com	auser@example.com	A message	Delivered successfully	0.6KB	
□	✉	17 Jun 2010 13:05:50	admin@example.com	admin@example.com	MailMarshal Receiver will slow down	Delivered successfully	1.0KB	
Viewing records 1 to 5 of 6 total messages							2.1MB	

4. In the results list, you can take action on one message, or on multiple messages. To show options for processing multiple messages, expand the **Bulk Actions** section of the page.

   a. To see additional details of a message, click ?.

b. Click the **Message Viewer** icon to examine the message content including attachments, and the processing log (if available). From this window you can process or reprocess a quarantined message.



http://spe.marshal.com - Message Viewer - Microsoft Internet Explorer

Message Details

To:	aexample@example.com	Date:	27 April 2007 08:20:58
From:	auser@not-here.com	Size:	130.3 KB
Subject:	For Example		

Type: Mail Body Size: 661 B

Cras purus. Aenean enim elit, venenatis eget, commodo non, tincidunt porta, lectus. Integer mattis, felis lacinia dictum elementum, nulla orci tristique eros, vitae rhoncus neque mi vitae eros. Ut imperdiet nisl sed magna. In hac habitasse platea dictumst. Vestibulum eu pede. Aenean varius eleifend neque. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Sed auctor tellus id arcu. Etiam sed pede. Suspendisse potenti. In a libero. Ut vitae ligula in purus pulvinar aliquam. Aliquam molestie sollicitudin erat. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae;

***Note:** For security reasons, the Message Viewer does not render images or HTML links in the browser. You can choose to download images.*

c. For messages that have not been delivered, click the **Process** icon to process or reprocess the message. You can choose to delete or retain messages that you process.

d. For messages that have been reprocessed, click the **Info** icon to see details of the action taken.

e. To take action on multiple messages, select the messages using the checkboxes at the left of the list, and then select a **Bulk Action**.

f. To export the list of messages, click **Download Results**.

For additional details of the Message Viewer, Bulk Actions, and Process windows, see **Help**.

GENERATING REPORTS

Within MailMarshal SPE Reports, reports are organized into four sub menus: system reports, configuration reports, billing reports, and scheduled reports. The MailMarshal SPE Reports allow you to generate reports based on the information that MailMarshal SPE logs as it processes email messages. You can choose from a wide range of reports covering business development and configuration. You can produce both overall summaries and per-customer or per-reseller details.

Note: *Detailed reports on messages processed for customers are available in the customer Web Console view for each customer. For details of these reports, see the User Guide and the Web Console Help. To log in to the customer Web Console, use the support login. See "Administrative Logins" on page 56.*

The Report screen is shown as a HTML page for viewing. Clicking the "Printer Friendly Version" button on the top bar produces a popup window ready for printing.

Available Reports

System Reports

Provides a list of reports associated with MailMarshal SPE, customers and their domains.

Report Name	Formats	Description
Arrays Reload History	Text	Lists times when policy changes were sent to MailMarshal SMTP arrays.
Configuration Checker	Text	Provides a quick overview of setup completeness for each array.
Customer Configuration Checker	Text	Provides a quick overview of features enabled for each customer.
Customer Policy Checker	Text	Provides a quick overview of policy types applied to each customer.
Customers Due to Expire	Text	Lists expiration dates for customer accounts.
Domain Status	Text	Lists average sender queue length for selected domains
Expired Customers	Text	Lists any customers whose subscription has expired.
Growth Reports	Text Graphic	Shows historical data on customers, managed email accounts, and managed domains.
License Allocation History	Text Graphic	Shows daily historical data on customer users consuming each type of sub-license (anti-virus, anti-spam, and content scanning).
License Allocation Summary	Text	Shows a current snapshot of customer users consuming each type of sub-license

Report Name	Formats	Description
MailMarshal Array License Key Information	Text	Provides details of the MailMarshal SMTP License Key installed on each array.
Service Levels	Text Graphic	Shows performance and disk availability over the selected period.

Configuration Reports

Lists reports for finding incorrect customer configurations and policy rules that may affect inbound/outbound emails.

Report Name	Formats	Description
Customer Checker	Text	Shows MX record status fro each domain.
Suspect Rules	Text	Shows rules that have large numbers of criteria or actions.

Billing Reports

Summarizes MailMarshal SPE licenses and usage.

Report Name	Formats	Description
Billing By Message	Text	Shows the configured and actual users for each domain.
Billing Configured	Text	Shows licenses and trials for each customer.
License Enforcement	Text	Provides details of license count enforcement options and status for each customer.
Reseller Detail	Text	Shows detailed information about customers assigned to each reseller.
Reseller Summary	Text Graphic	Shows a history of information about customers assigned to a specific reseller, or all resellers.

Scheduled Reports

This option is available once MailMarshal SPE Reporting Agent is installed. It allows you to send emails containing system, configuration and billing reports on a daily, weekly, fortnightly, or monthly schedule. To set up Scheduled Reports, see **Help** for this item.

Entering Report Parameters

You can customize many of the reports by entering parameters. Not all parameters area available for all reports. Some common parameters are described below. For more details, see the **Help** for each report.

Reporting Period

You can select the period in any of 5 ways, each represented by a tab. When entering a date, click the calendar icon at the right of the date field to view a calendar control.

Email To

Specify an email address to receive a copy of this report.

Output Type

Certain reports are available in both text and graphic. Choose the report type from the drop down box.

Array

Specify a specific array or server to report on, or choose All Arrays to see information about the entire MailMarshal SPE installation.

To generate a report with parameters:

1. Select the report tree from left pane of the Administration Console.
2. Double click the report name.
3. MailMarshal SPE displays a parameter detail pane. Specify the appropriate values.
4. Click **Submit** to view the report.

VIEWING CUSTOMER INFORMATION

Some information specific to customers can only be viewed from within the Customer Web Console. This include detailed message reports.

MailMarshal SPE creates two special administrative accounts with privilege to log in to the Customer Web Console. For details, see “Administrative Logins” on page 56.

To log in to the Customer Web Console:

1. Make a note of a domain that MailMarshal SPE manages for the customer.
2. Log in to the Customer Web Console using that domain and a login with Support Login or Site Login privilege. For example, to log in with read only access to the Customer Web Console for XYZ Corp, you can use the login `sitesupport@xyz.com`.

THE DASHBOARD

MailMarshal SPE includes a Dashboard window that provides an overview of server health and processing statistics. The information covers MailMarshal SPE and MailMarshal SMTP services, queues, traffic volume, viruses and spam detected, classifications, and quarantined messages.

To view the Dashboard, select **System Status > Dashboard** in the left pane. For details of the available options, see Help.

MONITORING AGENT SERVICES

MailMarshal SPE generates alerts for specific events of interest. Some of the events included are Agent services starting, stopping, or remaining idle for a longer than expected time.

To view a historical list of service alerts, select **System Status > Agent Status** in the left pane. You can expand the section for each Agent to see specific historical status information.

MONITORING ARRAY AND SERVER STATUS

MailMarshal SPE lists the servers in MailMarshal SMTP email processing infrastructure. It divides the sections into Array Status and Server Status.

To access the Array Status page, select **System Status > Array Status** in the left pane of the Administration Console. The Array Status page shows the current status of MailMarshal Array Managers registered with MailMarshal SPE, as well as MailMarshal SMTP version information.

You can view details of the Windows event logs on the array by clicking the link **Event Viewer** at the top left.

You can view details of the message queues, Receiver and Sender activity on the array by clicking the links **Message Queues**, **Receiver Threads**, and **Sender Threads** at the top left.

To access the Server Status page, select **System Status > Server Status** in the left pane of the Administration Console.

The server status page shows current state of the MailMarshal SMTP email processing servers. You can also see the state of the associated services and queues. The Receiver, Engine, and Sender services are shown with a green check (healthy) or red X (problems). You can view details of the message queues on the array from the Array Status page.

USING MAILMARSHAL SPE LOGS

Event Logs

Each component of MailMarshal SPE 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 the Event Log in the Web Console, navigate to **System Status > Array Status**, and then click the link **Event Viewer** at the top right.

Text Logs

Each MailMarshal SPE component generates text logs. These files provide a 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 installation folder of the corresponding components.

Verbose logging can be enabled by turning on Debug mode for each component under the MailMarshal SPE Windows Registry Key.

Warning: *Verbose logging should only be enabled if advised by M86 Technical Support. Verbose logging should not be left active during normal production use, as the log files may grow extremely large and use all available disk space. Enable this mode only as required, and disable it when not actively using it.*

The MailMarshal SPE Windows Registry Key is as follows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Marshal\MailMarshalSPE
```

The following subkeys may be available, depending on which software components have been installed.

- DatabaseWizard
- MaintenanceAgent

- ReplicationAgent
- ReportingAgent
- StatusAgent

To enable Debug mode for a component:

1. Using Windows Registry Editor, navigate to the subkey
2. If necessary, create a DWORD value `Debug`
3. To enable verbose logging, assign a value of 1. To disable debugging, assign a value of 0.

Email Processing Logs

When a MailMarshal 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 Customer Web Console. for more information, see the *User Guide.*

USING WINDOWS TOOLS

MailMarshal provides information in a standard format through the Windows event log and performance monitor.

Event Log

Each component of MailMarshal SMTP and MailMarshal SPE 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.

Performance Monitor

Each core service of MailMarshal SMTP (the Engine, Receiver, and Sender) makes several counters available to the Windows Performance Monitor.

Please see the documentation for Performance Monitor to learn more about its capabilities, which include remote monitoring. You can use Performance Monitor on a workstation to view performance of multiple servers.

Appendix A
Wildcards and Regular Expressions

MailMarshal SPE supports a simple wildcard syntax when you enter several types of information including user groups and Mail History parameters.

WILDCARD CHARACTERS

MailMarshal SPE allows wildcard entries in the following contexts:

- User Group items. See “Configuring User Groups” on page 116.
- Mail History search. See “Using Mail History” on page 221.
- Virus names in virus scanner results. See “Where the result of a virus scan is” on page 175.

In each of these types of entry, MailMarshal 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

Character	Function
[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 *etc.*
*.mail[0-9].ourcompany.com	mail5.ourcompany.com *but not* maila.ourcompany.com
mail[!0-9].ourcompany.com	mails.ourcompany.com *but not* 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 SPE uses regular expressions in header matching and rewriting rules. For more information about these rules, see “Standard Rules” on page 168.

MailMarshal SPE 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 Knowledge Base article Q10520.

This appendix provides limited information about some commonly used features and some extensions specific to MailMarshal SPE.

Shortcuts

The arrow to the right of each field on the matching 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.
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.
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.

Selection	Inserts	Usage
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 236.
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 SPE 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 SPE substitutes the second value. If the search expression does not match the first value in any line, MailMarshal SPE 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.

Input Email Address	Result
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

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.

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.

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, in Windows 2000 or later 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.

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 2000 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 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.

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. An internet based service that provides information about email sources. Typically used to filter spam. See also DNS Blacklist.

scalability. Ability to distribute loads across multiple servers, allowing for greater accessibility and balanced traffic.

service account. In Windows NT and Windows 2000, a user account that a service uses to log on to Windows NT or Windows 2000. 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.

SpamCensor. The proprietary spam detection technology incorporated in MailMarshal. SpamCensor includes a multi-faceted message analysis tool and regular definition updates.

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 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 2000 or later provides an X.500 directory service.

XML. See Extensible Markup Language (XML).

Index