LevelBlue

Secure What's Next.

MailMarshal

User Guide

November 2026



Legal Notice

Copyright © 2026 Trustwave Holdings, Inc.

The most current version of this document may be obtained from:

Support.LevelBlue.com/MailMarshal-SMTP/

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Format and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
`Code`	Text in this format indicates computer code or information at a command line.
Italics	Italics are used to denote the name of a published work, the current document, or another document; for text emphasis; or to introduce a new term. In code examples italics indicate a placeholder for values and expressions.
[Square brackets]	In code examples, square brackets indicate optional sections or entries.
	**Note:** This symbol indicates information that applies to the task at hand.
	**Tip:** This symbol denotes a suggestion for a better or more productive way to use the product.
	**Caution:** This symbol highlights a warning against using the product in an unintended manner.

Copyright © 2026 Trustwave Holdings, Inc.

Table of Contents

Legal Notice . . . . . **ii**

Formatting Conventions . . . . . **iii**

List of Tables . . . . . **xiv**

List of Figures . . . . . **xv**

1 Introduction **15**
1.1 What Is MailMarshal SMTP? 15
1.2 What Does MailMarshal SMTP Provide? 16
1.3 How MailMarshal SMTP Helps You 17
1.3.1 Filters Email at the Gateway 17
1.3.2 Delivers Layered Spam Protection 17
1.3.3 Protects Against Existing and Emerging Threats 17
1.3.4 Provides Unparalleled Performance 18
1.3.5 Includes Easy-to-Use Interfaces 18
1.4 How MailMarshal SMTP Works 18
1.4.1 Understanding What MailMarshal Does 19
1.4.2 Configuring MailMarshal 20
1.4.3 Monitoring and Reporting 20
1.5 MailMarshal SMTP and MailMarshal Cloud 21

2 Planning Your MailMarshal Installation **22**
2.1 Planning Checklist 22
2.2 Understanding MailMarshal Components 23
2.2.1 MailMarshal Components 23
2.2.2 Other Software and Services 24
2.3 Understanding Installation Scenarios 24
2.3.1 Standalone Installation 25
2.3.1.1 MailMarshal as Email Server 25
2.3.1.2 MailMarshal as an Internal Email Relay 26
2.3.1.3 MailMarshal on Existing Email Server 26
2.3.2 Array Installation 27
2.4 Hardware and Software Requirements 29
2.4.1 Standalone Installation Requirements 29
2.4.2 Array Installation Requirements 31
2.4.2.1 Server Requirements 31
2.4.2.2 Array Manager Requirements 33
2.4.3 Web Components Requirements 34
2.5 Database Software Considerations 35
2.6 Understanding MailMarshal Folder Locations 36

Copyright © 2026 Trustwave Holdings, Inc.

2.7 Supported Antivirus Software . . . 37
2.8 Collecting Information for Installation . . . 38

3 Installing and Configuring MailMarshal . . . 40
3.1 Installation Checklist . . . 40
3.2 Installing Prerequisite Software . . . 40
3.3 Installing MailMarshal on a Standalone Server . . . 41
3.4 Installing MailMarshal as an Array . . . 42
3.4.1 Installing a MailMarshal Array Manager . . . 42
3.4.2 Installing a MailMarshal Server . . . 46
3.5 Running the Configuration Wizard . . . 48
3.6 Configuring Email Routing . . . 52
3.7 Creating Directory Connectors . . . 53
3.8 Configuring Antivirus Scanning . . . 54
3.8.1 Excluding Working Folders From Virus Scanning . . . 55
3.8.2 Configuring MailMarshal to Use an Antivirus Product . . . 56
3.9 Installing and Customizing Web Components . . . 57
3.9.1 Installing the MailMarshal Web Components . . . 57
3.9.2 Customizing the Web Components . . . 59
3.10 Upgrading MailMarshal . . . 60
3.10.1 Upgrading from MailMarshal Version 10.1.0 or Above . . . 60
3.10.2 Upgrading from Other Versions of MailMarshal . . . 61
3.11 Uninstalling MailMarshal . . . 61

4 Understanding MailMarshal Interfaces . . . 63
4.1 Understanding the MailMarshal Web User Interface . . . 63
4.1.1 Working With the Dashboard and Status pages . . . 64
4.1.2 Working With Menu and Detail Items . . . 65
4.1.3 Working With Properties Configuration . . . 65
4.1.4 Committing Configuration . . . 66
4.1.5 Change Auditing . . . 66
4.1.6 Managing Authorized Users . . . 66
4.1.7 Understanding Email Management . . . 67
4.2 Understanding the Spam Quarantine Management Website . . . 68
4.3 Understanding Other Tools . . . 68

5 Implementing Your Email Content Security Policy . . . 70
5.1 Configuring Email Content Security . . . 70
5.2 Stopping Spam . . . 71
5.2.1 Anti-Spam Configuration and Rules . . . 71
5.2.2 Configuring SpamProfiler . . . 72
5.2.3 Configuring SpamCensor, SpamProfiler, and YAE Updates . . . 73
5.2.3.1 Configuring and Checking Automatic SpamCensor Updates . . . 73
5.2.3.2 Configuring Proxy Settings for Updates . . . 74
5.3 Stopping Viruses and Malware . . . 75

Copyright © 2026 Trustwave Holdings, Inc.

5.3.1 How MailMarshal Uses Virus Scanners . . . 75
5.3.1.1 Features . . . 75
5.3.1.2 Implementation Options . . . 76
5.3.2 Anti-Malware Policy and Rules . . . 76
5.3.3 Best Practices . . . 76
5.3.4 Viewing Virus Scanner Properties . . . 77
5.4 Preventing Relaying . . . 77
5.5 Controlling Who Can Send Email Through Your Server . . . 78
5.5.1 Reputation Services and DNS Blocklists . . . 78
5.5.1.1 Recommended Usage . . . 79
5.5.1.2 Configuring Access to a Reputation Service . . . 79
5.5.1.3 Using a Reputation Service Rule . . . 79
5.5.2 PTR Lookups . . . 80
5.5.3 Blocked Hosts . . . 80
5.5.4 Authentication by Account . . . 81
5.6 Preventing Malicious Email Attacks . . . 81
5.6.1 Understanding Denial of Service Attack Prevention . . . 81
5.6.1.1 How MailMarshal Prevents Attacks . . . 81
5.6.1.2 Optimizing DoS Attack Prevention Settings . . . 82
5.6.2 Preventing Denial of Service Attacks . . . 82
5.6.3 Enabling and Disabling DoS Attack Prevention . . . 83
5.6.4 Understanding Directory Harvest Attack Prevention . . . 83
5.6.4.1 How MailMarshal Prevents Attacks . . . 83
5.6.4.2 DHA Prevention Settings . . . 84
5.6.5 Preventing Directory Harvest Attacks . . . 84
5.6.6 Enabling and Disabling Directory Harvest Attack Prevention . . . 86
5.7 Filtering Messages and Attachments . . . 86

6 Understanding Email Policy, Policy Groups, and Rules . . . 88
6.1 Understanding Policy Types . . . 88
6.1.1 Connection Policy . . . 88
6.1.2 Content Analysis Policy . . . 88
6.1.3 Dead Letter Policy . . . 88
6.2 Understanding Policy Groups . . . 89
6.3 Understanding Rules . . . 90
6.3.1 Creating Rules . . . 90
6.4 Understanding User Matching . . . 92
6.5 Understanding Rule Conditions . . . 94
6.5.1 Rule Conditions for Content Analysis Policy Rules . . . 94
6.5.1.1 Where message is/is not detected as spam by SpamEngine . . . 95
6.5.1.2 Where the result of a virus scan is/is not . . . 96
6.5.1.3 Where message is/is not identified as containing malware by Yara Analysis Engine 98
6.5.1.4 Where message does/does not contain suspect URLs . . . 98
6.5.1.5 Where message does/does not appear to be spoofed based on criteria . . . 98

Copyright © 2026 Trustwave Holdings, Inc.

6.5.1.6 Where message did/did not trigger TextCensor script(s) 100
6.5.1.7 Where message attachment is/is not of type 100
6.5.1.8 Where attachment fingerprint is/is not known 101
6.5.1.9 Where message does/does not contain attachments named 101
6.5.1.10 Where attachment parent is of type 102
6.5.1.11 Where the attached image does/does not/may match image category 102
6.5.1.12 Where message size is 104
6.5.1.13 Where the estimated bandwidth required to deliver this message is 104
6.5.1.14 Where message attachment size is 105
6.5.1.15 Where number of recipients is count 105
6.5.1.16 Where number of attachments is count 105
6.5.1.17 Where the sender is/is not in the recipient's safe senders list 105
6.5.1.18 Where the sender is/is not in the recipient's blocked senders list 106
6.5.1.19 Where sender's IP address does/does not match address 106
6.5.1.20 Where sender did/did not authenticate successfully 107
6.5.1.21 Where message was/was not received via TLS 107
6.5.1.22 Where message was/was not received via TLS versions 107
6.5.1.23 Where the TLS client certificate was/was not presented with criteria 107
6.5.1.24 Where the external command is/is not triggered 107
6.5.1.25 Where message does/does not contain one or more headers 107
6.5.1.26 Where message does/does not trigger category script(s) 108
6.5.1.27 Where the DKIM verification result is 109
6.5.1.28 Where message was checked with DMARC and a result applied 109
6.5.2 Rule Conditions for Connection Policy Rules 109
6.5.2.1 Where message is of a particular size 109
6.5.2.2 Where SPF evaluation result is 110
6.5.2.3 Where sender's HELO name is/is not criteria 110
6.5.2.4 Where sender's IP address does/does not match address 110
6.5.2.5 Where sender did/did not authenticate successfully 111
6.5.2.6 Where sender's IP address is/is not listed by Reputation Service 111
6.5.2.7 Where message was/was not received via TLS 111
6.5.2.8 Where message was/was not received via TLS versions 112
6.5.2.9 Where the TLS client certificate was/was not presented with criteria 112
6.5.3 Rule Conditions for Dead Letter Policy Rules 112
6.5.3.1 Where the Dead Letter reason contains 112
6.5.3.2 Where message is detected as spam by SpamProfiler 112
6.6 Understanding Rule Actions 112
6.6.1 Rule Actions for Content Analysis Policy Rules 112
6.6.1.1 Send a notification message 114
6.6.1.2 Log message with classifications 114
6.6.1.3 Copy the message 114
6.6.1.4 Report the DMARC Policy Disposition 114
6.6.1.5 Do not generate an NDR if the remote host refuses the message 114
6.6.1.6 Run the external command 115
6.6.1.7 Add attachments to valid fingerprints list 115

Copyright © 2026 Trustwave Holdings, Inc.

6.6.1.8 Add message users into group . . . 115
6.6.1.9 Stamp message with text . . . 115
6.6.1.10 Strip attachment . . . 116
6.6.1.11 Rewrite message headers . . . 116
6.6.1.12 Prepend text to message subject . . . 116
6.6.1.13 Rewrite URLs in the message for Blended Threat Scanning . . . 116
6.6.1.14 Send a copy of the message to host . . . 117
6.6.1.15 BCC a copy of the message . . . 117
6.6.1.16 Deliver the mail via TLS only . . . 117
6.6.1.17 Set message routing to host . . . 118
6.6.1.18 Ignore DANE validation . . . 118
6.6.1.19 Apply DKIM signature . . . 118
6.6.1.20 Move the message and categorize . . . 118
6.6.1.21 Park the message . . . 119
6.6.1.22 Hold the message . . . 119
6.6.1.23 Delete the message . . . 119
6.6.1.24 Pass the message to rule . . . 119
6.6.1.25 Continue processing . . . 120
6.6.2 Rule Actions for Connection Policy Rules . . . 120
6.6.2.1 Accept message . . . 120
6.6.2.2 Refuse message and reply with message . . . 120
6.6.2.3 Continue Processing Rules . . . 121
6.6.3 Rule Actions for Dead Letter Policy Rules . . . 121
6.6.3.1 BCC a copy of the message . . . 121
6.6.3.2 Send a notification message . . . 122
6.6.3.3 Write log message(s) with classifications . . . 122
6.6.3.4 BCC a copy of the message . . . 122
6.6.3.5 Set message routing to host . . . 122
6.6.3.6 Move the message . . . 123
6.6.3.7 Delete the message . . . 123
6.6.3.8 Pass message through to recipients . . . 123
6.7 Understanding the Order of Evaluation . . . 123
6.7.1 Adjusting the Order of Evaluation of Policy Groups . . . 123
6.7.2 Adjusting the Order of Evaluation of Rules . . . 124
6.8 Viewing Email Policy . . . 124

7 Understanding Email Policy Elements . . . 125
7.1 Configuring Connectors . . . 126
7.2 Configuring User Groups . . . 127
7.2.1 Creating and Populating User Groups . . . 127
7.2.1.1 Adding Members to a MailMarshal Group . . . 128
7.2.1.2 Adding Groups to a MailMarshal Group . . . 128
7.2.1.3 Pruning a MailMarshal Group . . . 128
7.2.2 Moving and Copying Users and Groups . . . 129
7.3 Configuring IP Groups . . . 129

Copyright © 2026 Trustwave Holdings, Inc.

7.3.1 Creating and Populating IP Groups . . . 129
7.3.1.1 Adding Members to an IP Group . . . 129
7.3.1.2 Editing an IP Group Member . . . 130
7.3.1.3 Adding Groups to an IP Group . . . 130
7.3.2 Moving and Copying IP Groups . . . 130
7.4 Identifying Email Text Content Using TextCensor Scripts . . . 130
7.4.1 TextCensor Elements . . . 130
7.4.1.1 Wildcards . . . 130
7.4.1.2 Positional Operators . . . 131
7.4.1.3 Logical (Boolean) and Special Operators . . . 132
7.4.1.4 Anchored Regular Expressions . . . 133
7.4.2 TextCensor Concepts . . . 134
7.4.2.1 Words . . . 134
7.4.2.2 Phrases . . . 134
7.4.2.3 Symbols and Punctuation . . . 134
7.4.2.4 Word Breaks . . . 134
7.4.2.5 Accented Letters . . . 135
7.4.2.6 Escape Characters . . . 135
7.4.2.7 Case Sensitivity . . . 135
7.4.2.8 Classes . . . 135
7.4.2.9 Named Statements . . . 136
7.4.3 Scoring a TextCensor Script . . . 136
7.4.4 Creating Scripts . . . 137
7.4.5 Editing Scripts . . . 139
7.4.6 Duplicating Scripts . . . 140
7.4.7 Importing Scripts . . . 140
7.4.8 Exporting Scripts . . . 140
7.4.9 TextCensor Best Practices . . . 141
7.4.9.1 Constructing TextCensor Scripts . . . 141
7.4.9.2 Decreasing Unwanted Triggering . . . 141
7.4.10 Testing Scripts . . . 142
7.5 Notifying Users with Message Templates and Message Stamps . . . 142
7.5.1 Message Templates . . . 142
7.5.2 Creating a Message Template . . . 143
7.5.3 Creating Digest Templates . . . 144
7.5.4 Editing Templates . . . 146
7.5.5 Duplicating Templates . . . 147
7.5.6 Deleting Templates . . . 147
7.5.7 Working with Message Stamps . . . 147
7.5.7.1 Duplicating Message Stamps . . . 148
7.5.7.2 Editing Message Stamps . . . 148
7.5.7.3 Deleting Message Stamps . . . 148
7.5.8 Using Variables . . . 148
7.5.9 Date Formatting . . . 153
7.6 Using Virus Scanning . . . 154

Copyright © 2026 Trustwave Holdings, Inc.

7.7 Using Folders and Message Classifications 154
7.7.1 Working with Message Classifications 154
7.7.1.1 Editing Message Classifications 155
7.7.1.2 Duplicating Message Classifications 155
7.7.1.3 Deleting Message Classifications 155
7.7.2 Working with Folders 155
7.7.3 Creating Folders 156
7.7.4 Editing Folders 157
7.7.4.1 Deleting Folders 157
7.7.4.2 Configuring Default Folder Access 157
7.7.4.3 Configuring Access for a Specific Folder 158
7.8 Header Matching and Rewriting 159
7.8.1 Changing and Adding Headers with the Receiver 159
7.8.2 Using Rules to Find Headers 159
7.8.3 Using Rules to Change Headers 160
7.8.4 Using the Header Rewrite Editor 160
7.9 Extending Functionality Using External Commands 163
7.10 Configuring Reputation Services 165

8 Monitoring Email Flow 166
8.1 Using the MailMarshal Console for Email Management 167
8.1.1 Connecting to MailMarshal Using the Console 167
8.1.2 Monitoring Email Statistics and Server Health 167
8.1.3 Deleting and Retrying Queued Messages 168
8.1.4 Viewing Folders and Folder Contents 168
8.1.5 Working With Email Messages 169
8.1.5.1 Forwarding Messages 169
8.1.5.2 Deleting Messages 170
8.1.5.3 Restoring Messages 170
8.1.5.4 Viewing Messages 170
8.1.5.5 Releasing Messages 172
8.1.6 Viewing Email History 173
8.1.7 Searching Folders and Email History 174
8.1.8 Searching Rejected Messages 175
8.1.9 Auditing Quarantine Actions 175
8.1.10 Viewing Alert History 175
8.1.11 Viewing Event History 176
8.1.12 Finding Events 176
8.1.12.1 Event Log Filter 176
8.1.12.2 Event Log Search 176
8.2 Using Windows Tools 177
8.2.1 Event Log 177
8.2.2 Performance Monitor 178
8.3 Using MailMarshal Text Logs 178

Copyright © 2026 Trustwave Holdings, Inc.

9 Managing MailMarshal Configuration. 179
9.1 Managing Your MailMarshal Licenses 179
9.1.1 Reviewing Installed Licenses and Maintenance 179
9.1.2 Requesting a New License Key 180
9.1.3 Entering a License Key 180
9.2 Backing Up and Restoring the Configuration 181
9.2.1 Backing Up the Configuration 181
9.2.2 Automatic Configuration Backup 182
9.2.3 Restoring the Configuration 182
9.3 Configuring Local Domains 183
9.3.1 Changing Local Domains Information 184
9.4 Configuring Routes 185
9.4.1 Editing Routing Table Information 185
9.4.2 Marking Routes as Down 187
9.5 Configuring Relaying 188
9.5.1 Editing Relay Table Information 188
9.6 Configuring Delivery Options 189
9.6.1 Configuring Default Delivery Options 189
9.6.2 Configuring Delivery Options For A Specific Server 190
9.7 Setting Up Accounts 191
9.7.1 Creating Accounts 191
9.7.2 Editing Existing Accounts 192
9.7.3 Deleting Accounts 192
9.8 Configuring Email Batching 192
9.9 Configuring DKIM 193
9.10 Configuring DMARC 194
9.11 Managing Array Nodes 195
9.11.1 Managing Node Services 195
9.11.2 Adding and Deleting Nodes 195
9.11.2.1 Adding a Node 195
9.11.2.2 Deleting a Node 196
9.11.3 Joining a Node to an Array 196
9.11.4 Customizing Settings for Nodes 196
9.12 Understanding Secure Email Communications 197
9.13 Securing Email Communications 198
9.13.1 Working with Certificates 198
9.13.2 Securing Inbound Communications 199
9.13.3 Securing Outbound Communications 200
9.14 Setting Advanced Options 200
9.14.1 MailMarshal Properties – Advanced 200
9.14.2 Advanced Settings 202
9.14.3 Setting Up Syslog Integration 202
9.14.4 Setting Up Azure Information Protection Integration 203
9.14.5 Setting Node Properties – Advanced 203
9.14.6 Working with Array Communications 204

Copyright © 2026 Trustwave Holdings, Inc.

9.14.6.1 Changing Array Port Settings . . . 204
9.14.6.2 Changing the Database Location . . . 204
9.14.7 Changing Folder Locations . . . 205
9.15 Using the Group File Import Tool . . . 205
9.15.1 Group File Import Text File Format . . . 206
9.15.2 Group File Import Command Format . . . 206
9.16 Using the Configuration Export Tool . . . 207
9.16.1 Export Configuration Command Format . . . 207
9.17 Using the Configuration Converter Tool . . . 208
9.18 Using the Config Service Admin Tool . . . 209

10 Delegating Spam and Quarantine Management . . . 210
10.1 Setting Up Console Access . . . 210
10.2 Setting Up Spam Quarantine Management Features . . . 210
10.2.1 Spam Quarantine Management Windows . . . 211
10.2.2 Setting Up Folders and Templates . . . 212
10.2.3 Setting Up Message Digests . . . 213
10.2.3.1 Creating Message Digests . . . 213
10.2.3.2 Editing Message Digests . . . 214
10.2.3.3 Deleting Message Digests . . . 214
10.2.4 Setting Up Rules . . . 214
10.2.5 Setting Up Spam Quarantine Management for Other Folders . . . 214
10.3 Using the Message Release External Command . . . 215
10.3.0.1 Message Release Options . . . 216

11 Reporting on MailMarshal Activity . . . 218
11.1 Data Retention and Grouping . . . 218
11.1.1 Configuring Data Retention . . . 218
11.1.2 Configuring Reporting Groups . . . 219

Appendix A: Wildcards and Regular Expressions . . . 220
A.1 Wildcard Characters . . . 220
A.2 Regular Expressions . . . 221
A.2.1 Shortcuts . . . 222
A.2.2 Reserved Characters . . . 222
A.2.3 Examples . . . 223
A.2.4 Map Files . . . 224

Appendix B: Third Party Extensions . . . 225
B.1 Image Analyzer . . . 225
B.1.1 Why Would I Use Image Analyzer? . . . 225
B.1.2 What Results Can I Expect From Image Analyzer? . . . 225
B.1.3 How Does Image Analyzer Address the Issues? . . . 226
B.2 Virus Scanning Software . . . 226

Glossary . . . 227

Copyright © 2026 Trustwave Holdings, Inc.

Index **233**

Copyright © 2026 Trustwave Holdings, Inc.

List of Tables

Table 1: MailMarshal component functions . . . 19
Table 2: Planning checklist . . . 22
Table 3: Standalone installation requirements . . . 30
Table 4: Array Server installation requirements . . . 31
Table 5: Array Manager Server requirements . . . 33
Table 6: Web Components Server requirements . . . 34
Table 7: Sample database worksheet . . . 35
Table 8: Database worksheet for your environment . . . 35
Table 9: Database sizing calculations . . . 36
Table 10: Supported Antivirus scanners . . . 38
Table 11: Information required for installation . . . 38
Table 12: Installation checklist . . . 40
Table 13: Variables for message description . . . 121
Table 14: TextCensor Positional Operators . . . 131
Table 15: TextCensor Logical and Special Operators . . . 132
Table 16: TextCensor Regular Expression Operators . . . 133
Table 17: TextCensor Classes . . . 135
Table 18: Cumulative scoring options . . . 137
Table 19: Digest detail levels . . . 144
Table 20: Digest options . . . 144
Table 21: MailMarshal variables . . . 149
Table 22: Date formatting variables . . . 153
Table 23: Email monitoring options . . . 166
Table 24: Files to include in configuration backup . . . 181
Table 25: Group File Import file syntax . . . 206
Table 26: Group File Import command options . . . 207
Table 27: Configuration Export Tool command options . . . 208
Table 28: Wildcard syntax . . . 220
Table 29: Wildcard example results . . . 221
Table 30: Regular Expression shortcuts . . . 222
Table 31: Map file example results . . . 224

Copyright © 2026 Trustwave Holdings, Inc.

List of Figures

Figure 1: MailMarshal components . . . 23
Figure 2: MailMarshal as email server . . . 25
Figure 3: MailMarshal as email relay . . . 26
Figure 4: MailMarshal installed on internal email server . . . 26
Figure 5: MailMarshal Array installation . . . 28
Figure 6: Spam Quarantine Management configuration page . . . 59
Figure 7: Management Console Dashboard . . . 64
Figure 8: Management Console Status . . . 65
Figure 9: Management Console Folders . . . 67
Figure 10: Spam Quarantine Management website . . . 68
Figure 11: Virus scanning rule condition . . . 97
Figure 12: Message spoofing analysis rule condition . . . 99
Figure 13: Image analysis rule condition . . . 103
Figure 14: Category script rule condition . . . 108
Figure 15: Message window . . . 171
Figure 16: Release Message window . . . 172
Figure 17: Event log search window . . . 177

Copyright © 2026 Trustwave Holdings, Inc.

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.

1.1 What Is MailMarshal SMTP?

MailMarshal SMTP – previously known as Trustwave Secure Email Gateway (SEG) – is a fast, easy-to-use email content security solution that ensures a safe and productive working environment by enforcing your Acceptable Use Policy and protecting against spam, viruses, and other undesirable content.

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

Key elements of the MailMarshal anti-spam solution include:

- **SpamProfiler,** an antispam pre-filter that can reject spam email without unpacking and full processing.
- **SpamCensor,** an advanced antispam engine that can filter most spam before it enters your network.
- **SpamBotCensor,** an optimized application of SpamCensor that can block spam generated by botnets with even greater efficiency.
- **Yara Analysis Engine (YAE),** a scripted anti-malware engine to perform deep analysis of messages and attachments.
- **Automatic updates** for SpamProfiler, SpamCensor, and YAE, responding to the latest trends in Spam.
- **Zero Day updates** protecting you from significant spam and malware events.

Copyright © 2026 Trustwave Holdings, Inc.

- **URLCensor**, to reject email based on URLs embedded in messages that are listed on a DNS based blocklist.
- **URL checking** for suspect URLs using a real-time lookup against a database maintained by Level-Blue.
- **TextCensor**, to analyze and filter inbound and outbound messages based on language content.

MailMarshal is a gateway product that can be used with any internal company email system or cloud hosted mailbox offering, including Microsoft Exchange, Office 365/Exchange Online, Lotus Domino, Sendmail, and Linux email servers. MailMarshal provides your company with the layered security solution you need to manage email content, fight spam, and transparently enforce your email Acceptable Use Policy.

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

1.2 What Does MailMarshal SMTP Provide?

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

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

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

- Attempted message delivery from a server found on a blocklist
- Presence of a virus (using one or more supported virus scanners)
- Presence of particular phrases in header, message, or attachment
- Size or type of attachments
- Presence of URLs in header, message, or attachment that are found on a DNS based blocklist

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

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

Copyright © 2026 Trustwave Holdings, Inc.

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

Management Console

Allows email security administrators to configure the product and establish email policy. Also allows email administrators and help desk personnel to monitor and control product activity, and administer quarantined email.

Spam Quarantine Management Website

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

1.3 How MailMarshal SMTP Helps You

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

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

1.3.1 Filters Email at the Gateway

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

1.3.2 Delivers Layered Spam Protection

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

1.3.3 Protects Against Existing and Emerging Threats

MailMarshal integrates a wide variety of anti-spam and anti-threat technology to protect against known threats, as well as regular updates to meet emerging threats. The LevelBlue Labs team continually updates threat detection algorithms to detect new forms of spam, mass mailing worms, and phishing scams. MailMarshal can automatically download these updates to keep your protection levels current. The LevelBlue Labs team also publishes Zero Day updates to meet specific threats.

Copyright © 2026 Trustwave Holdings, Inc.

The MailMarshal IP Reputation Service provides real-time updates of a proprietary database of spam-related email servers.

1.3.4 Provides Unparalleled Performance

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

1.3.5 Includes Easy-to-Use Interfaces

MailMarshal is easy to evaluate, install, and use. Default settings provide excellent anti-spam performance “out of the box.”

The Management Console provides an intuitive web-based interface that allows both policy configuration and email management. Policy administrators can refine the rules MailMarshal uses to evaluate and reject or deliver email. Email administrators can monitor product effectiveness and manage quarantined messages.

An optional Web-based end user management console allows email users to review quarantined email, and establish and manage personal rules for acceptable and unacceptable email. These user interfaces allow various users to easily access the information they need about the MailMarshal solution.

Auditors and managers can easily produce reports on MailMarshal activity using the optional web-based Marshal Reporting Console.

1.4 How MailMarshal SMTP Works

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

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

MailMarshal provides one main user interface (the Management Console), as well as an optional end-user Spam Quarantine Management site.

Copyright © 2026 Trustwave Holdings, Inc.

1.4.1 Understanding What MailMarshal Does

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

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

Table 1: MailMarshal component functions

Receiver Functions	Engine Functions	Sender Functions
• Inbound TLS • SMTP Authentication • Blocked Hosts • Relaying Tables • DoS Protection • DHA Protection • Reputation Services (DNS Blocklists) • Global Header Rewriting • Connection Policy (Receiver Rules) • DKIM, SPF, DMARC, and ARC-SEAL Evaluation • SpamProfiler rejection	• Content Analysis Policy (Standard Rules) • Malware Scanning • SpamBotCensor • SpamProfiler and SpamCensor quarantining • SpamCensor advanced usage (spam types) • NDRCensor • Suspect URL Check • Blended Threats URL Rewriting • Message Archiving • Route Message To Host • Message Parking • DKIM and ARC-SEAL Signing • Azure Information Protection RMS decryption	• Domain Routing Tables • Outbound TLS • DANE validation • MTA-STS validation • SMTP Authentication

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

Next, the MailMarshal Engine unpacks each email, expanding any attached archive or compressed files. The Engine then checks each component against Content Analysis 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 rules by changing the rule order and by changing specific characteristics of the rule.

MailMarshal also scans email for viruses using antivirus scanning software. MailMarshal supports several integrated scanners with high-throughput interfaces. The product can also use many other

Copyright © 2026 Trustwave Holdings, Inc.

antivirus scanners that return results in the required format. However, non-integrated scanners deliver much lower throughput.

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 Sender for delivery to the appropriate recipients. The sender can enforce use of TLS and DANE validation.
- Modified email can be delivered to recipients with attachments removed.
- Virus-laden email is quarantined.

MailMarshal 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.

1.4.2 Configuring MailMarshal

You configure MailMarshal rules and settings using the Management Console web interface. Changes made and committed in the Management Console are applied through the MailMarshal Array Manager. The Array Manager coordinates the activity of all other MailMarshal Servers in the array and connects with the user interfaces, optional end user quarantine management server, and the database.

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

1.4.3 Monitoring and Reporting

The Management Console features the Dashboard to summarize MailMarshal activity and server health at a glance. Using the Console, email administrators can review email processing history for a message and view and release any quarantined message.

The administrator can grant other users access to specific Console functions. Using this feature, the administrator can delegate basic tasks to help desk or departmental personnel. The Management Console is web-based to allow remote access.

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

Administrators and managers can generate reports on MailMarshal activity using Marshal Reporting Console. Marshal Reporting Console uses SQL Server Reporting Services to produce reports. This is a server application with a website interface. Marshal Reporting Console can deliver reports by web view, email, FTP, or local network files, and can schedule automatic delivery of reports.

Marshal Reporting Console is provided as a separate package from LevelBlue. This application is available to all MailMarshal customers.

Copyright © 2026 Trustwave Holdings, Inc.

1.5 MailMarshal SMTP and MailMarshal Cloud

MailMarshal SMTP is a gateway solution that applies email content security for email inbound from or outbound to the Internet. MailMarshal Cloud is a cloud based solution that applies the power of MailMarshal in a managed cloud solution compatible with cloud based mail providers or premise solutions.

For more information about MailMarshal Cloud, see the documentation available on the LevelBlue website.

Copyright © 2026 Trustwave Holdings, Inc.

2 Planning Your MailMarshal Installation

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

2.1 Planning Checklist

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

Table 2: Planning checklist

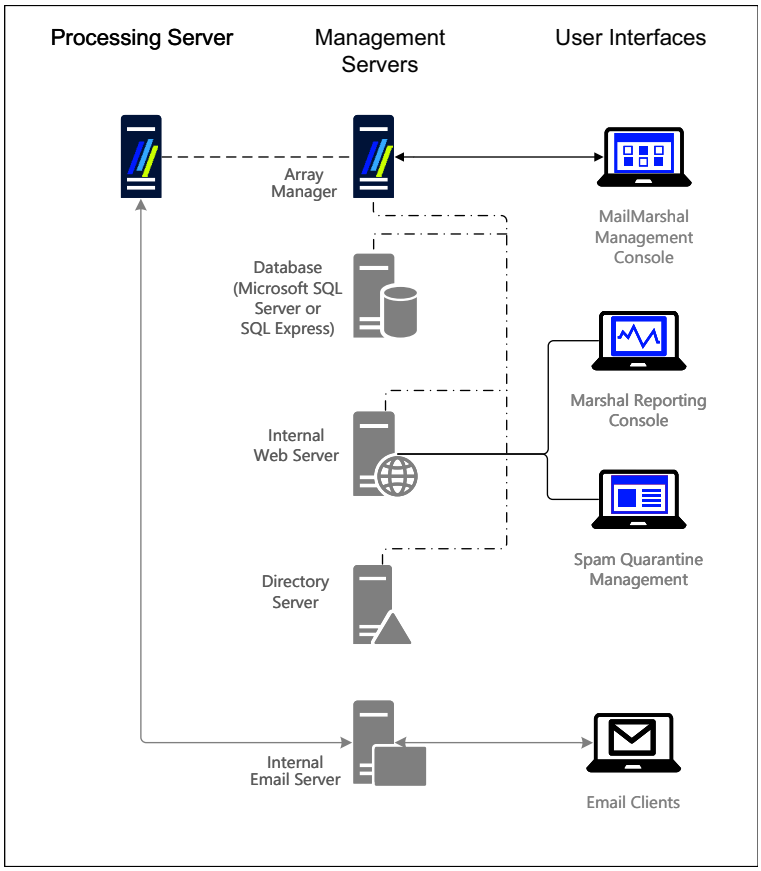
☑	Step	See Section
☐	1. Learn about important MailMarshal concepts.	"Understanding MailMarshal Components" on page 23.
☐	2. Choose a *standalone* or *array* installation.	"Understanding Installation Scenarios" on page 24.
☐	3. *If you selected a standalone installation,* choose the appropriate configuration for your environment.	"Standalone Installation" on page 25.
☐	4. *If you selected an array installation,* determine the number and location for the MailMarshal Servers and Array Manager components.	"Array Installation" on page 27.
☐	5. Ensure the computers meet the hardware and software requirements.	"Standalone Installation Requirements" on page 29 or "Array Installation Requirements" on page 31
☐	6. Determine whether to use Microsoft SQL Server or SQL Express (or Azure SQL for Azure installations).	"Database Software Considerations" on page 35.
☐	7. Decide where to install the MailMarshal folders.	"Understanding MailMarshal Folder Locations" on page 36.
☐	8. Choose the antivirus software to use with MailMarshal.	"Supported Antivirus Software" on page 37.
☐	9. Collect installation information about your email environment.	"Collecting Information for Installation" on page 38.

Copyright © 2026 Trustwave Holdings, Inc.

2.2 Understanding MailMarshal Components

MailMarshal consists of several software components, which you can install on different computers in your network. These components can be installed in a variety of configurations to suit any size organization from small businesses to distributed enterprises. Figure 1 shows the components on separate computers for clarity. In lower volume scenarios you can install all components on a single computer.

Figure 1: MailMarshal components



2.2.1 MailMarshal Components

MailMarshal includes the following components:

Processing Server

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

Array Manager

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

Copyright © 2026 Trustwave Holdings, Inc.

Express. The Array Manager server also hosts the Configuration Service and an instance of Microsoft IIS, used by the Management Console. For more information, see “Other Software and Services” on page 24.

Management Console

Web-based interface allowing Administrator access. Administrators can define policy (rules), configure MailMarshal, and manage and monitor undelivered or filtered email.

Spam Quarantine Management Website

Optional Web-based interface for internal email users to view and manage quarantined email.

Marshal Reporting Console

Optional Web-based interface used to generate traffic and management reports based on MailMarshal activity.

To operate properly, MailMarshal requires an Array Manager (with Management Console), at least one email processing Server, and a database server (hosting the product database and configuration service database). You can optionally install the Spam Quarantine Management website and the Marshal Reporting Console if you plan to use the additional features these components offer.

2.2.2 Other Software and Services

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

Microsoft SQL Server, SQL Express, or Azure SQL Server

The MailMarshal database stores configuration data and log information. If your email volume permits, you can use the free SQL Express. If your email volume is higher, use Microsoft SQL Server. If possible, install the database software and the MailMarshal Array Manager on the same computer. For more information, see “Array Installation Requirements” on page 31 and “Database Software Considerations” on page 35.

If your MailMarshal installation is hosted on an Azure server, you can use Azure SQL to host the database. Due to latency, you should not attempt to use Azure SQL with a locally hosted MailMarshal installation.

Microsoft Internet Information Services (Microsoft IIS)

If you want to offer the end-user Spam Quarantine Management Website, install the MailMarshal Web Components on a server with Microsoft IIS and .NET (3.5 SP1 and 4.6) installed.

2.3 Understanding Installation Scenarios

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

- Standalone, or basic installation (several variations available)

Copyright © 2026 Trustwave Holdings, Inc.

- Array installation

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

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

For more information about determining your configuration needs, see the Technical Reference titled "MailMarshal Sizing Guide" at LevelBlue.com, or contact your Technical Support representative.

2.3.1 Standalone Installation

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

To use the MailMarshal Spam Quarantine Management Website or Marshal Reporting Console, install these components on a Microsoft IIS Server.

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

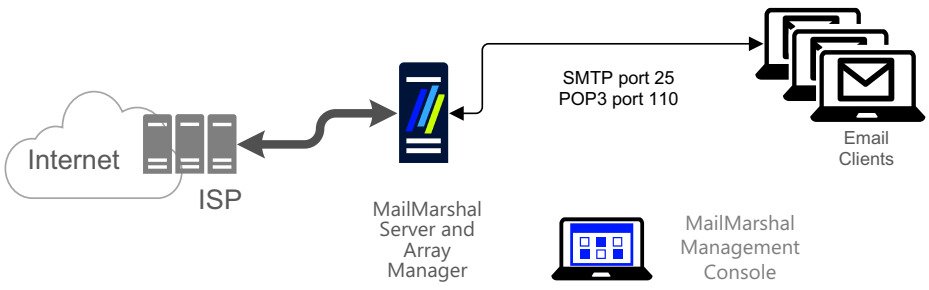
- As a POP3/SMTP server *(for very small organizations)*
- As an internal email relay to your email server
- On your existing email server

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

2.3.1.1 MailMarshal as Email Server

You can install MailMarshal to function as a POP3/SMTP email server, providing all email server functions for a small organization, as shown in Figure 2.

Figure 2: MailMarshal as email server



Copyright © 2026 Trustwave Holdings, Inc.

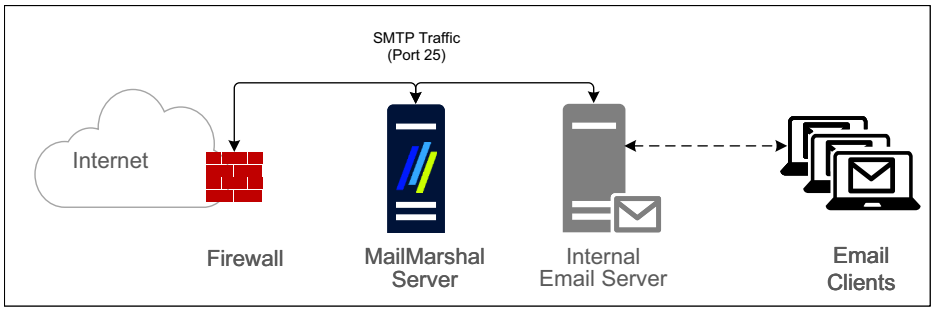
In this scenario, MailMarshal receives and processes all incoming email. MailMarshal receives email on port 25 from within the organization and delivers email to internal POP3 mailboxes on port 110. MailMarshal receives and sends email to and from external addresses over your Internet link.

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

2.3.1.2 MailMarshal as an Internal Email Relay

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

Figure 3: MailMarshal as email relay



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

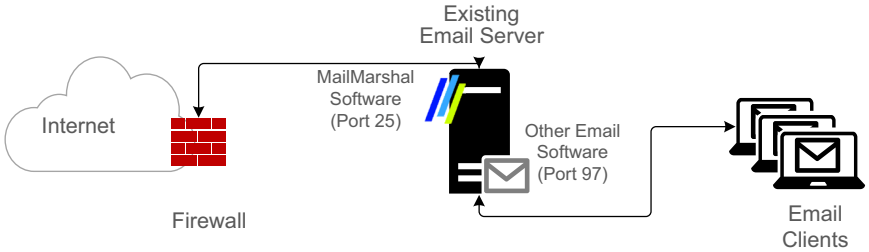
For this configuration, install the MailMarshal Server and Array Manager components on a separate computer from the existing email server. Set the Domain Name Service Mail Exchange (DNS MX) records or firewall relay settings so the MailMarshal Server receives all inbound email.

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

2.3.1.3 MailMarshal on Existing Email Server

You can install MailMarshal on your existing email server computer, as shown in the following figure.

Figure 4: MailMarshal installed on internal email server



Copyright © 2026 Trustwave Holdings, Inc.

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

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

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

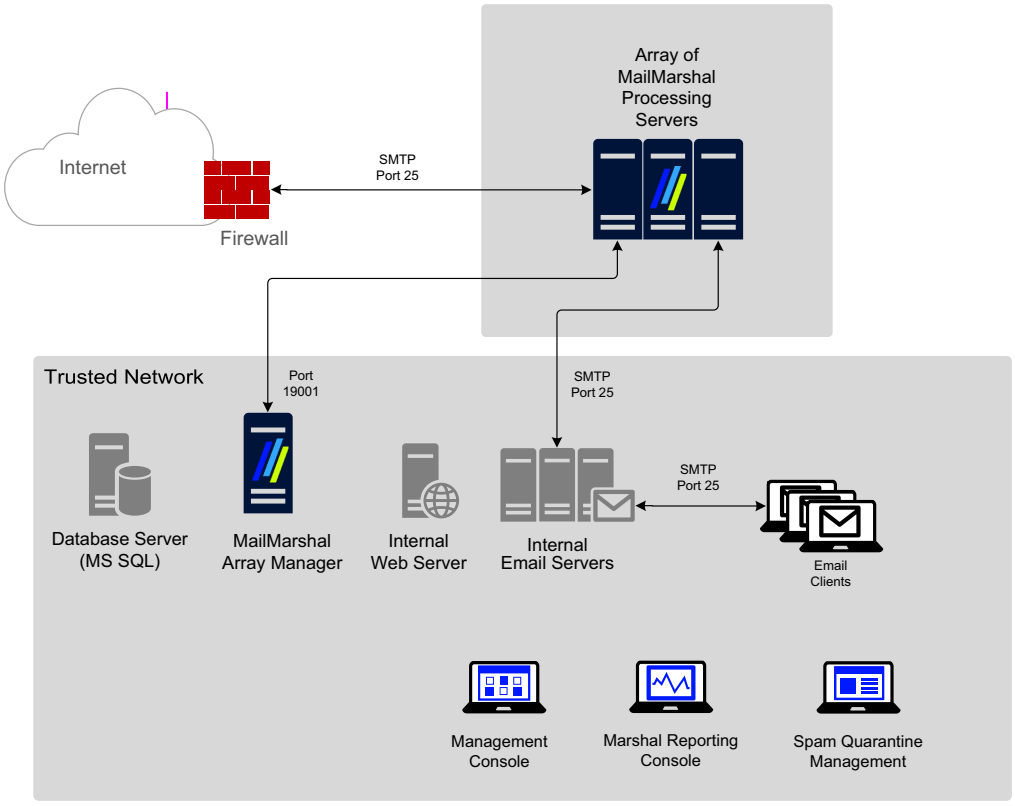
This configuration is not suitable if you have multiple internal email servers (SMTP or Exchange). With multiple internal email servers, install MailMarshal on a separate computer as an email relay. For more information, see “MailMarshal as an Internal Email Relay” on page 26.

2.3.2 Array Installation

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

Copyright © 2026 Trustwave Holdings, Inc.

Figure 5: MailMarshal Array installation



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

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

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

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

Install the MailMarshal Array Manager, and the database if possible, on a dedicated computer inside the trusted network. The location of the Array Manager can affect the performance of the

Copyright © 2026 Trustwave Holdings, Inc.

administration and configuration tools used in MailMarshal, but does not affect email processing performance.

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

- On the same server as the Microsoft SQL Server hosting the database. Since the Array Manager is the only MailMarshal component that communicates directly with the database, installing the Array Manager on the computer that hosts Microsoft SQL Server or SQL Express results in the most efficient operation.
- On another computer in the network close to the computer hosting the database over a high-speed network connection.
- On an Active Directory Global Catalog or other Directory Server. The Array Manager communicates regularly to the Global Catalog if you are running Active directory, or through LDAP to another existing Directory Server.
- The MailMarshal Management Console website is installed on the Array Manager server and can be accessed by web browser clients.
- To use the MailMarshal Spam Quarantine Management Website or Marshal Reporting Console, install these components on a Microsoft IIS Server domain member inside the network.

2.4 Hardware and Software Requirements

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

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

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

For more information about the latest requirements and supported environments, see the LevelBlue Knowledgebase.

2.4.1 Standalone Installation Requirements

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

Copyright © 2026 Trustwave Holdings, Inc.

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

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

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

Table 3: Standalone installation requirements

Category	Requirements
Processor	**Minimum**: Core i5 or similar performance
Disk Space	**Minimum**: 20GB (NTFS)
Memory	**Minimum**: 7GB (Includes 1 GB for operating system and 2GB for SQL) • Minimum 5 GB if the database is hosted on another server
Supported Operating System	• Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Essentials Edition or above • Windows 11 (Only for smaller installations and not recommended)
Network Access	• TCP/IP protocol • Domain structure • External DNS name resolution: DNS MX record to allow MailMarshal Server to receive inbound email
Software	• Microsoft .NET Framework 4.6.2 (or later 4.X) •.NET 10 is also used but is included in the MailMarshal installer • Microsoft IIS for Management Console. •Windows Authentication is required. • Database server: *Use of full licensed SQL Server is not recommended for standalone installations due to resource contention issues.* Use SQL 2025 Express, SQL 2022 Express, SQL 2019 Express, or SQL 2017 Express. For cloud installations you can use Azure SQL Server. For more information about database considerations, see “Database Software Considerations” on page 35. SQL Server versions have additional prerequisites, including minimum Operating System versions. • Antivirus scanning software supported by MailMarshal. For more information, see “Supported Antivirus Software” on page 37. • Web browser (for Management Console connection): Chrome, Edge, Firefox, or Safari.

Copyright © 2026 Trustwave Holdings, Inc.

Table 3: Standalone installation requirements

Category	Requirements
Port Access	• Port 25: Inbound SMTP and to email servers • Port 53: for DNS external email server name resolution (TCP and UDP) • Port 80 (HTTP) and Port 443 (HTTPS) outbound: for SpamCensor and SpamProfiler updates, and CRL checking for TLS if TLS is in use (Proxy usage is supported) • Port 443 (HTTPS) inbound: for client connections to the MailMarshal Management Console • Port 1433: for connection to SQL Server database and Marshal Reporting Console computers • If installed on an existing email server: Port 97 or another available port, for email transfer between MailMarshal and the other software • If serving as a POP3 email server: Port 110, for email transfer to POP3 mailboxes

When processing large volumes of email, disk I/O can become a limitation. To provide optimal throughput in this case, plan to include dual drives so you can install the MailMarshal Server components on one drive and the database and Unpacking folder on a separate physical drive. For more information about choosing folder locations, see “Understanding MailMarshal Folder Locations” on page 36.

To provide redundancy, plan for quad drives configured as two mirrored pairs. For more information to determine your configuration needs, see the Technical Reference titled “MailMarshal Sizing Guide” at LevelBlue.com.

2.4.2 Array Installation Requirements

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

For more information to determine your specific requirements, see the “MailMarshal Sizing Guide” Technical Reference, at LevelBlue.com.

2.4.2.1 Server Requirements

The following table lists system requirements for a MailMarshal email processing server computer in an array configuration.

Table 4: Array Server installation requirements

Category	Requirements
Processor	**Minimum**: Core i5 or similar performance
Disk Space	**Minimum**: 20GB (NTFS)

Copyright © 2026 Trustwave Holdings, Inc.

Table 4: Array Server installation requirements

Category	Requirements
Memory	**Minimum**: 10GB (includes 2GB for operating system)
Supported Operating System	• Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Essentials Edition or above • Windows 11 (Only for smaller installations and not recommended)
Network Access	• TCP/IP protocol • Domain structure • DNS service available
Software	• Microsoft .NET Framework 4.6.2 (or later 4.X) • Antivirus scanning software supported by MailMarshal. For more information, see “Supported Antivirus Software” on page 37. • Web browser (for Management Console connection): Chrome, Edge, Firefox, or Safari.
Port Access	• Port 25: Inbound SMTP and email forwarding to email servers in trusted network • Port 53: DNS external email server name resolution (TCP and UDP) • Port 80 (HTTP) and Port 443 (HTTPS): for SpamProfiler updates, and CRL checking for TLS if TLS is in use (Proxy usage is supported) • Port 19001: Communication with MailMarshal Array Manager in the trusted network

When processing large volumes of email, disk I/O can become a limitation. To provide optimal throughput in this case, you may want to plan for dual drives in the MailMarshal Server computer so you and install Server components on one drive and the Unpacking folder on a separate physical drive. For more information about choosing folder locations, see “Understanding MailMarshal Folder Locations” on page 36.

To provide redundancy, you may want to plan for quad drives configured as two mirrored pairs. For more information about determining your configuration needs, see the “MailMarshal Sizing Guide” Technical Reference at LevelBlue.com

Copyright © 2026 Trustwave Holdings, Inc.

2.4.2.2 Array Manager Requirements

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

Table 5: Array Manager Server requirements

Category	Requirements
Processor	**Minimum**: Core i5 or similar performance
Disk Space	**Minimum**: 20GB (NTFS) and additional space depending on database retention
Memory	**Minimum**: 10GB (includes 2GB for operating system and 2GB for SQL)
Supported Operating System	• Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Essentials Edition or above • Windows 11 (Only for smaller installations and not recommended)
Network Access	• TCP/IP protocol • Domain structure • DNS service available
Software	• Microsoft .NET Framework 4.6.2 (or later 4.X) •.NET 10 is also used but is included in the MailMarshal installer • Microsoft IIS for Management Console •Windows Authentication is required • Database server: SQL 2025, SQL 2022, SQL 2019, SQL 2017; SQL 2025 Express, SQL 2022 Express, SQL 2019 Express, SQL 2017 Express. Azure SQL Server can be used where MailMarshal is installed on Azure. For more information about database considerations, see “Database Software Considerations” on page 35. SQL Server versions have additional prerequisites, including minimum Operating System versions. • Antivirus scanning software supported by MailMarshal. For more information, see “Supported Antivirus Software” on page 37.
Port Access	• Port 80 (HTTP) and Port 443 (HTTPS) outbound: SpamCensor updates (Proxy usage is supported) • Port 443 (HTTPS) inbound: Client access to the MailMarshal Management Console website • Port 1433: Connection from Marshal Reporting Console computers • Port 19001: Communication with MailMarshal Servers in DMZ • Port 19006 (HTTPS): Communication from any applications using the REST API • Port 19007 (HTTPS): Communication from the MailMarshal Management Console or other applications using the MailMarshal Config Service

Copyright © 2026 Trustwave Holdings, Inc.

2.4.3 Web Components Requirements

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

Table 6: Web Components Server requirements

Category	Requirements
Processor	**Minimum**: Core i5 or similar performance
Disk Space	**Minimum**: 100MB **Recommended**: 500MB
Memory	**Minimum**: 512MB **Recommended**: 1024MB
Supported Operating System	• Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Essentials Edition or above • Windows 11 (Only for smaller installations and not recommended)
Network Access	• TCP/IP protocol • Domain structure • DNS service available
Software	• Microsoft .NET Framework 3.5.1 SP1 and 4.X • IIS Features (in addition to features installed by default): •ASP.NET •Basic Authentication •Windows Authentication
Web Browsers *(Tested and supported)*	• Microsoft Edge, Mozilla Firefox, Google Chrome, and Safari (current versions)
Port Access	• Port 19001: Communication with MailMarshal Array Manager

Use a secure (HTTPS) website to protect user data and authentication information.



Caution: As best practice for security, do not install the Spam Quarantine Management website on a server exposed to the Internet.

There are additional requirements to install Web components on a computer running a Windows Domain Controller. For more information, see the LevelBlue Knowledgebase.

Copyright © 2026 Trustwave Holdings, Inc.

2.5 Database Software Considerations

MailMarshal supports use of SQL Express or Microsoft SQL Server. To estimate the size of your MailMarshal database and determine whether to use SQL Express or Microsoft SQL Server, review the following sample worksheet, and then complete My Worksheet (Table 8 on page 35) with appropriate estimates.

Table 7: Sample database worksheet

Sample Worksheet		
Number of users	=	100
Average number of valid and quarantined email messages per user per day	x	70
Kilobytes per message or classification logged (1KB = 1000 Bytes)	x	2
Number of days in log data retention period	x	100
Safety margin	x	1.25
Total database size in Kilobytes for retention period	=	1,750,000 KB
Total database size in Gigabytes for retention period (divide by 1,000,000)	=	1.75 GB



Note: Each record in the Message table (quarantine, classification or delivery record) adds approximately 1.1KB to the database (depending on the size of data) Indexing on the Message table adds a smaller but significant amount. The Content table (logging of attachments) can also consume significant space, depending on the average number of attachments per message.

Table 8: Database worksheet for your environment

My Worksheet		
Number of users	=	
Average number of valid and quarantined email messages per user per day	x	
Kilobytes per message logged (1KB = 1000 Bytes)	x	3
Number of days in log data retention period	x	
Safety margin	x	
Total database size in Kilobytes for retention period	=	
Total database size in Gigabytes for retention period (divide by 1,000,000)	=	

Copyright © 2026 Trustwave Holdings, Inc.

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

Table 9: Database sizing calculations

Users	Email/Day/ User	Days to Keep Logs	Safety Margin	GB (Rounded)	Database Version
100	70	100	1.25	2	Express
200	70	100	1.25	3.5	Express
250	70	100	1.25	4.5	Express
500	70	100	1.25	9	Express
1000	70	100	1.25	20	SQL
2000	70	100	1.25	35	SQL
5000	70	100	1.25	90	SQL

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

If you have more than 500 email users, the Microsoft SQL Server memory footprint can become quite high. In this case, you can add memory to the Microsoft SQL Server computer (3GB or more) so Microsoft SQL Server can use its maximum available memory and still reserve memory for the Array Manager, operating system, and other system demand. Other environment factors may also affect performance and throughput rates. For large installations, consider using multiple disk drives for the various database files to optimize SQL Server performance.

Note: SQL Server, in particular 64 bit versions, will consume all available system memory by default. You may need to limit SQL memory usage. See Knowledgebase article Q14902.

2.6 Understanding MailMarshal Folder Locations

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

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

Copyright © 2026 Trustwave Holdings, Inc.

Logging

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



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

Queues

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

Unpacking

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

Quarantine

MailMarshal uses this folder as the default location for all quarantine folders. MailMarshal stores all quarantined messages in sub folders of this folder, including any archived messages, deadlettered messages that could not be processed fully, and messages in the Mail Recycle Bin. Ensure the disk drive where this folder resides has enough free space to accommodate the messages. The space required varies depending on your retention policies for quarantined messages. You can move individual folders to physically separate places on the server. For more information, see “Working with Folders” on page 155.



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

For more information, see Knowledgebase article Q11669.

2.7 Supported Antivirus Software

MailMarshal supports a number of third-party antivirus scanners to scan for virus or malware laden email. The scanners offering a MailMarshal specific DLL file offer much higher throughput and enhanced features. Command line scanners are suitable for basic scanning in relatively small organizations.

Copyright © 2026 Trustwave Holdings, Inc.

LevelBlue licenses the Marshal antivirus solutions separately from the MailMarshal product. Trial versions of the Marshal antivirus solutions are available from the installation package or as downloads from LevelBlue.com.

MailMarshal actively supports the antivirus software brands listed in the following table. For more information about currently supported versions, see Knowledgebase article levelblueQ10923.

Table 10: Supported Antivirus scanners

Antivirus Application	Features
Bitdefender for Marshal	DLL
McAfee for Marshal	DLL
Sophos for Marshal	DLL
Computer Associates AntiVirus (formerly eTrust EZAntiVirus or InoculateIT)	Command line scanner
McAfee Command Line	Command line scanner
NOD32 Command Line	Command line scanner

Notes:

- The Sophos (SAVI interface) and Symantec scanners that were previously supported are not supported in this release, as the required 64-bit integration is not currently available.
- Kaspersky for Marshal is no longer sold.

2.8 Collecting Information for Installation

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

Table 11: Information required for installation

Information required	My information
Names of computers where you plan to install MailMarshal components including: Servers, Array Manager/Management Console, database, and optionally, SQM and Marshal Reporting Console.	
Prerequisite software for each computer where you will install software and the best time to restart each system, if necessary.	
DNS server administrator of domains for which MailMarshal will process email and best time to make and propagate DNS changes.	
Firewall administrator contact information, and best time to make and propagate firewall settings changes.	

Copyright © 2026 Trustwave Holdings, Inc.

Table 11: Information required for installation

Information required	My information
Antivirus software to use with MailMarshal.	
Company name for MailMarshal license.	
Names of local domains for which MailMarshal will process email (for example, `mycompany.com` or `pop.mycompany.com`)	
IP address and access port for your existing Microsoft SQL server computer.	
IP address and access port for your existing local email server.	
If using POP3 mailboxes, decide how to route email for undefined accounts.	
Logon credentials for your directory server (Azure Entra, Active Directory or LDAP). IP address of the LDAP server.	
Email address where MailMarshal will send administrator notification emails (existing or new account).	
Email address email notifications to recipients will be from (reply to address) (existing or new account).	
IP addresses of primary and optional secondary DNS servers MailMarshal will use for internal and external domain name resolution.	
Server name, fully qualified domain name, or IP address of host and optional alternate to forward external email.	
Existing outbound delivery details and required routing changes.	
Existing inbound delivery details and required routing changes.	

Copyright © 2026 Trustwave Holdings, Inc.

3 Installing and Configuring MailMarshal

Before you install MailMarshal, be sure to complete the steps in the planning checklist. For more information, see “Planning Checklist” on page 22.

When you complete the planning checklist, you should know if you are planning a standalone or array installation, which MailMarshal components you want to install, and on which computers you plan to install each component. Collect the information listed in “Collecting Information for Installation” on page 38 before you run the Configuration Wizard.

If you are upgrading a MailMarshal installation from an earlier version, there are a number of other considerations. For more information, see “Upgrading MailMarshal” on page 60.

3.1 Installation Checklist

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

Table 12: Installation checklist

☑	Steps	See Section
☐	1. Install prerequisite software.	“Installing Prerequisite Software” on page 40
☐	2. *If you are installing MailMarshal on a standalone server,* install all components.	“Installing MailMarshal on a Standalone Server” on page 41
☐	3. *If you are installing MailMarshal on an array of servers,* install required components on each computer.	“Installing MailMarshal as an Array” on page 42
☐	4. Run the Configuration Wizard.	“Running the Configuration Wizard” on page 48
☐	5. Configure email routing as necessary to direct incoming mail to MailMarshal and mail delivery as needed.	“Configuring Email Routing” on page 52
☐	6. Create connections to your directory services to populate MailMarshal groups.	“Creating Directory Connectors” on page 53
☐	7. Configure MailMarshal to use your antivirus product.	“Configuring Antivirus Scanning” on page 54
☐	8. Optionally, install MailMarshal Spam Quarantine Management Web component.	“Installing and Customizing Web Components” on page 57

3.2 Installing Prerequisite Software

Before installing MailMarshal, install any prerequisite software the MailMarshal components require. This will simplify troubleshooting, and allow you to avoid restarting your computer during the product

Copyright © 2026 Trustwave Holdings, Inc.

installation process. For more information about required software for each MailMarshal computer in your configuration, see “Hardware and Software Requirements” on page 29.

The MailMarshal installation package includes many prerequisites, and provides links that allow you to download the remaining prerequisites from LevelBlue or vendor sites.

Note: To install the integrated virus scanning packages linked on the MailMarshal setup program Scanners tab, you must first install MailMarshal. The scanner installers check for a valid product license on the local server.

For information about antivirus configuration, see “Supported Antivirus Software” on page 37 and “Configuring Antivirus Scanning” on page 54.

To install prerequisite software or included antivirus products:

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

3.3 Installing MailMarshal on a Standalone Server

You can install the MailMarshal Server, Array Manager, and database on one computer. For more information about standalone MailMarshal installation, see “Standalone Installation” on page 25 and “Standalone Installation Requirements” on page 29

Use the **Basic Install** option to install MailMarshal on a standalone computer. The basic install option installs MailMarshal using the default installation and folder locations. If you are installing from the “with SQL Express” version of the installer package, the Basic Install installs a local instance of SQL Express if necessary. To use a different SQL Server computer, select **Custom Install**. See the instructions under “Installing a MailMarshal Array Manager” on page 42.

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

If you later want to specify alternate folder or database locations for MailMarshal, use the MailMarshal Server Tool. For more information, see “Changing Folder Locations” on page 205.

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

1. Ensure you have installed all prerequisite software specified for a standalone installation. For more information, see “Standalone Installation Requirements” on page 29 and “Installing Prerequisite Software” on page 40.
2. Log on to the computer as a member of the local Administrators group.
3. Close any open applications.
4. Run the setup program from the MailMarshal installation package.

Copyright © 2026 Trustwave Holdings, Inc.

5. On the Setup tab, click **Install MailMarshal**.
6. On the Welcome window, click **Next.**
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement,** and then click **Next.**
9. On the Setup Type window, select **Basic Install,** and then click **Next.**

   If you choose to install SQL Express:

   a. Note that SQL Express will install .NET Framework 4.6. The setup program prompts you to enter a strong password for the SQL Express **sa** account.

   b. SQL Express setup executes in silent mode. This process may take a number of minutes. Once installation is complete, MailMarshal installation continues.

10. The Basic Install process attempts to connect to a SQL instance on the local computer using Windows authentication, and create a database named `MailMarshal`.



Note: If the process encounters problems connecting, you can use Custom Install for more options. See the instructions under “Installing a MailMarshal Array Manager” on page 42. If the database already exists, you can choose to use or re-create it. If you are unsure, use Custom Install to create a database with a different name.

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

You must run the Configuration Wizard before MailMarshal can receive email and apply rules. For more information, see “Running the Configuration Wizard” on page 48.

3.4 Installing MailMarshal as an Array

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

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

Base the number of servers you install on your email volume. You can add servers later as needed. For more information about an array installation and requirements, see “Array Installation” on page 27 and “Array Installation Requirements” on page 31.

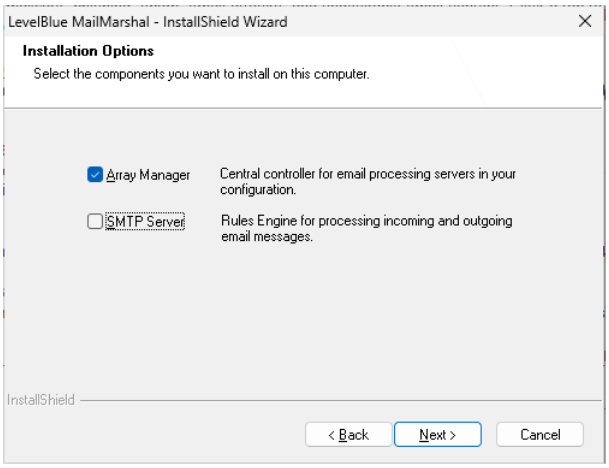
3.4.1 Installing a MailMarshal Array Manager

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

To install the Array Manager:

Copyright © 2026 Trustwave Holdings, Inc.

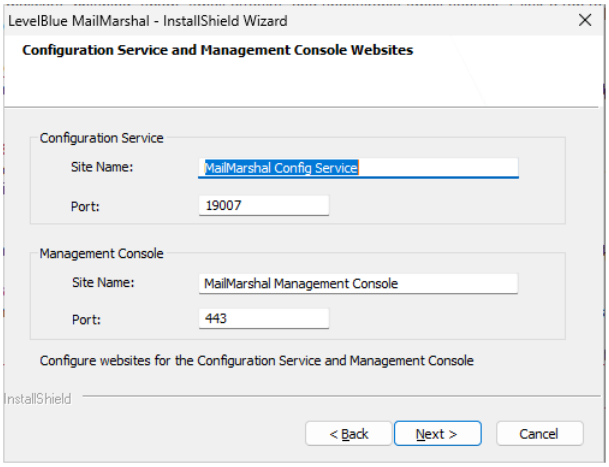
1. Ensure you have installed all prerequisite software specified for an array installation. For more information, see “Array Manager Requirements” on page 33 and “Installing Prerequisite Software” on page 40.
2. Log on to the computer as a member of the local Administrators group.
3. Close any open applications.
4. Run the MailMarshal installation package.
5. On the Setup tab, click **Install MailMarshal**.
6. On the Welcome window, click **Next.**
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement,** and then click **Next.**
9. On the Setup Type window, select **Custom Install,** and then click **Next.**
10. On the Installation Options window, ensure **Array Manager** is selected. The MailMarshal Management Console user interface is installed by default when you install the Array Manager component.
11. Clear **SMTP Server**, and then click **Next.** The installer verifies the presence of IIS, required for the Management Console website.



12. On the SQL Server Options window, choose to use an existing SQL server or install SQL Express locally (if the installation package includes SQL Express).
13. On the Choose Installation Location window, optionally change the installation and folder locations.

Copyright © 2026 Trustwave Holdings, Inc.

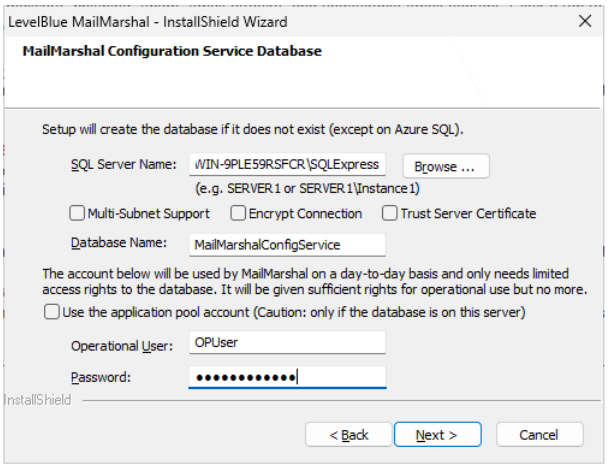
14. On the Configuration Services and Management Console Websites window, set site names and ports for the MailMarshal Configuration Service and Management Console websites.



15. On the Configuration Service Administrator window, specify a Windows username and password, full name and email address for the Config Service.

Note: These credentials are used as the initial login for the MailMarshal Management Console website. You can create other credentials after completing installation.

16. On the MailMarshal Configuration Service Database window, set SQL Server options for the MailMarshal Configuration Service database.



a. Specify a local or remote SQL server.

- If the endpoint is an Availability Group or Failover Cluster Instance, select Multi-Subnet Support to improve failover performance (see Microsoft documentation for details).
- If the endpoint is configured with encryption, select Encrypt Connection and Trust Server Certificate. For more information about encryption settings for SQL Server and MailMarshal, see Knowledgebase article levelblueQ21224.

Copyright © 2026 Trustwave Holdings, Inc.

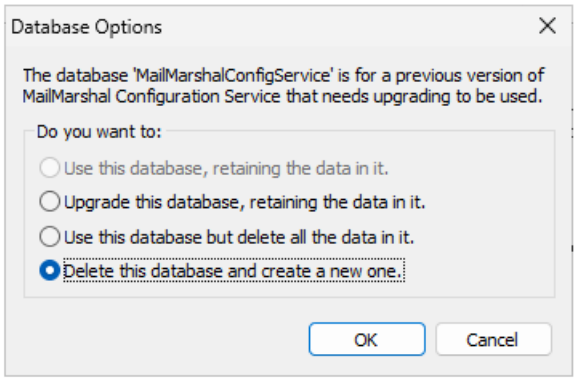
b. Specify a database name (by default, `MailMarshalConfigService`).

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

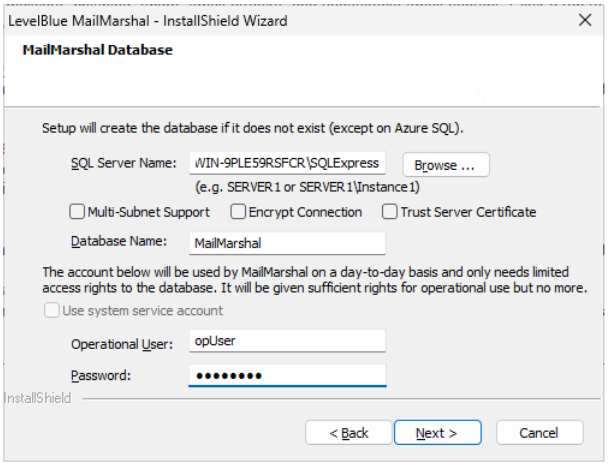
c. Choose an account to use for database access. This account can be a Windows or SQL Server account. If the SQL Server is on the same computer as MailMarshal, you can use the Application Pool account (the Application Pool Identity of the MailMarshal Management Console website).

Note: You can change the account information later using the MailMarshal Config Service Admin Tool.

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



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



a. Specify a local or remote SQL server.

- If the endpoint is an Availability Group or Failover Cluster Instance, select Multi-Subnet Support to improve failover performance (see Microsoft documentation for details).

Copyright © 2026 Trustwave Holdings, Inc.

- If the endpoint is configured with encryption, select Encrypt Connection and Trust Server Certificate. For more information about encryption settings for SQL Server and MailMarshal, see Knowledgebase article Q21224.

b. Specify a database name (by default, `MailMarshal`).

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

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

Note: You can change the account information later using the MailMarshal Server Tool.

19. Click **Next.** MailMarshal verifies the database information. If the database you selected already exists, you can choose options to use it, or cancel and provide a different database name. The available options depend on the database that is actually found.
20. Follow the instructions in the setup program until you finish installing MailMarshal.
21. On the Setup Complete window, ensure **Open the Management Console Website** is selected, and then click **Finish**. The Management Console opens in the default browser. The Management Console installs by default as the default HTTPS website of the local machine.

Notes:

- You cannot use Internet Explorer to access the Management Console.
- The HTTPS certificate that is automatically generated may be reported as invalid by some web browsers. You can configure another certificate using IIS.

You must complete the Configuration Wizard in the Management Console website before MailMarshal can receive email and apply rules. For more information, see "Running the Configuration Wizard" on page 48.

3.4.2 Installing a MailMarshal Server

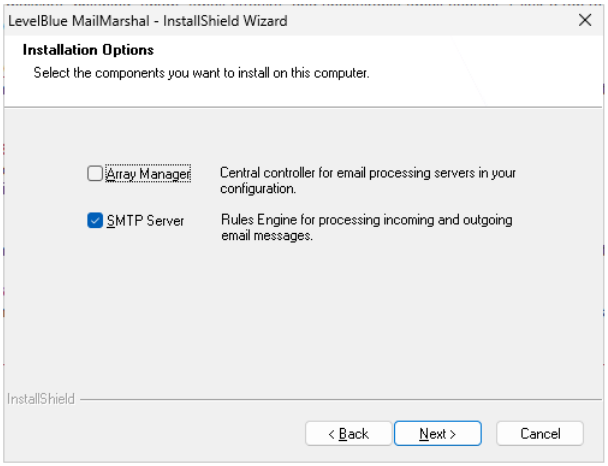
To complete a MailMarshal array installation, first install the MailMarshal Array Manager. Then, follow the steps to install a MailMarshal Server on additional computers. You can install additional email processing servers initially or add them later as needed.

To install the MailMarshal Server components:

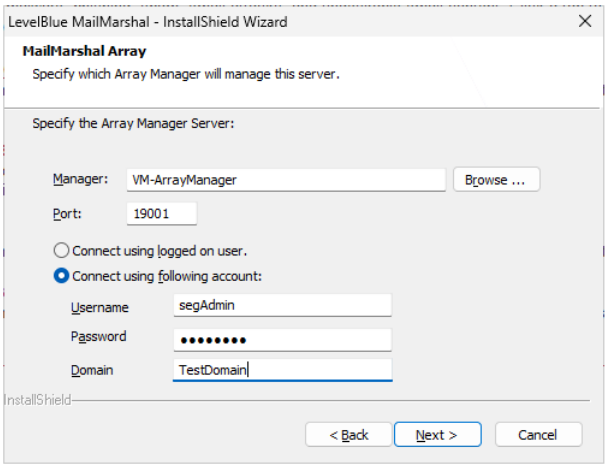
1. Ensure you have installed all prerequisite software specified for a MailMarshal Server computer. For more information, see "Server Requirements" on page 31 and "Installing Prerequisite Software" on page 40.
2. Log on to the computer you plan to use as a MailMarshal Server as a member of the local administrator group.

Copyright © 2026 Trustwave Holdings, Inc.

3. Close any open applications.
4. Run the setup program from the MailMarshal installation kit.
5. On the Setup tab, click **Install MailMarshal.**
6. On the Welcome window, click **Next.**
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement,** and then click **Next.**
9. On the Setup Type window, select **Custom Install,** and then click **Next.**
10. On the Installation Options window, ensure **SMTP Server** is selected.
11. Clear **Array Manager**, and then click **Next.**

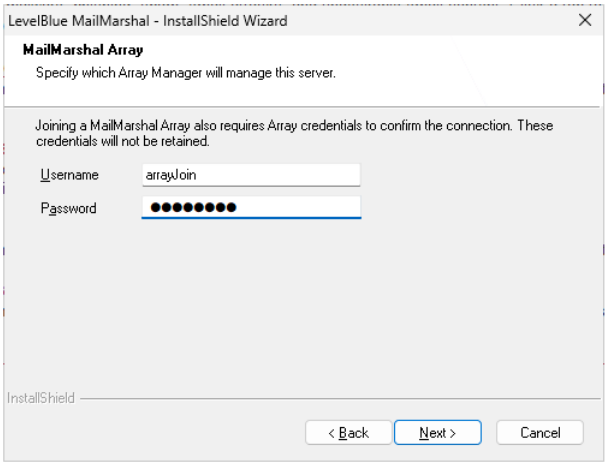


12. On the MailMarshal Array window, enter the name of the MailMarshal Array Manager that you will use to manage policy for this server. The name can be the computer name, IP address, or Fully Qualified Domain Name.
13. *If you have changed the default MailMarshal port,* enter the new value in the **Port** field.
14. *If you are not logged in as a user with permission to join the MailMarshal array,* select **Connect using following account** and enter Windows credentials with permission to connect to the Array Manager server.



Copyright © 2026 Trustwave Holdings, Inc.

15. Click **Next.**
16. Enter a MailMarshal Array Join credential. To create and administer these credentials, see the Array Join tab of the MailMarshal Server Tool on the Array Manager. Both the username and password are case sensitive. The default credential is:
    - Username: `arrayJoin`
    - Password: the server name of the Array Manager computer in uppercase



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

3.5 Running the Configuration Wizard

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

When you click **Finish** on the final window of the MailMarshal Setup Wizard, by default MailMarshal opens the Management Console website to the configuration wizard. If you do not run this wizard after running setup, MailMarshal runs the wizard the first time you access the MailMarshal Management Console.

Notes:

- You cannot use Internet Explorer to access the Management Console.
- The HTTPS certificate that is automatically generated may be reported as invalid by some web browsers. You can configure another certificate using IIS.

To run the Configuration Wizard:

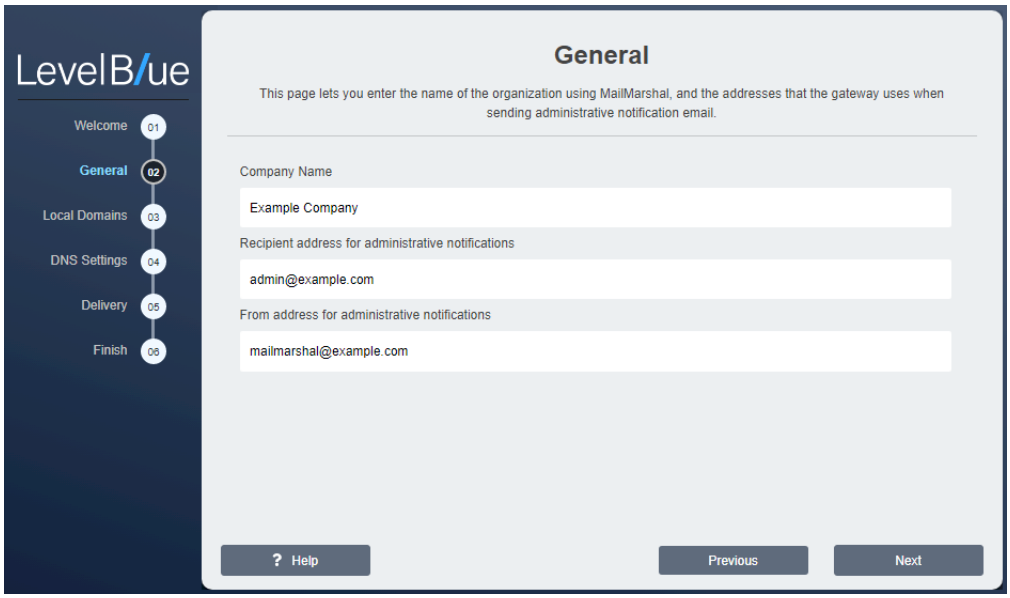
Copyright © 2026 Trustwave Holdings, Inc.

1. *If the Configuration Wizard is not running,* start the Wizard by browsing to the MailMarshal Management Console website. Use a supported browser (Chrome, Edge, Firefox, or Safari).
2. Log in to the Management Console. For a custom install use the Username and Password you entered in the Installation Wizard. For a basic install use Username `admin` and Password `admin`.



Note: For security, you should change the default password as soon as possible after completing the Wizard. See the Authorized Users item in the Management Console.

3. On the Welcome window, click **Next.**
4. On the General window:



   a. Type your company or organization name. This information identifies your organization when you request a license key for MailMarshal.

   b. Enter a **Recipient Address**. MailMarshal sends administrative notifications (such as Dead Letter reports) to the address you specify in this field. This address should be a valid and appropriate mailbox or group alias within the local delivery domains of MailMarshal.

   c. MailMarshal 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 within the local delivery domains of MailMarshal.

5. Click **Next**.
6. On the Local Domains window, enter one or more domain names for which this MailMarshal server will accept incoming mail.

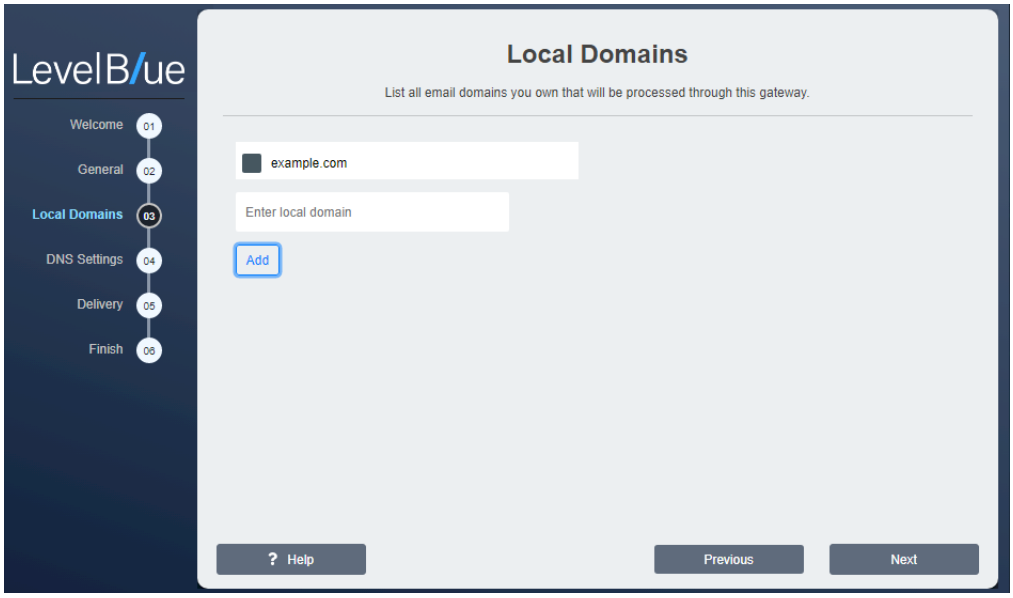
   a. Enter a domain name, and then click **Add**.

   b. Repeat the above steps for each local domain

   c. To delete an existing entry, select it and then click **Remove**.

   d. To change an entry, delete it and then add it again.

Copyright © 2026 Trustwave Holdings, Inc.



7. Click **Next**.

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

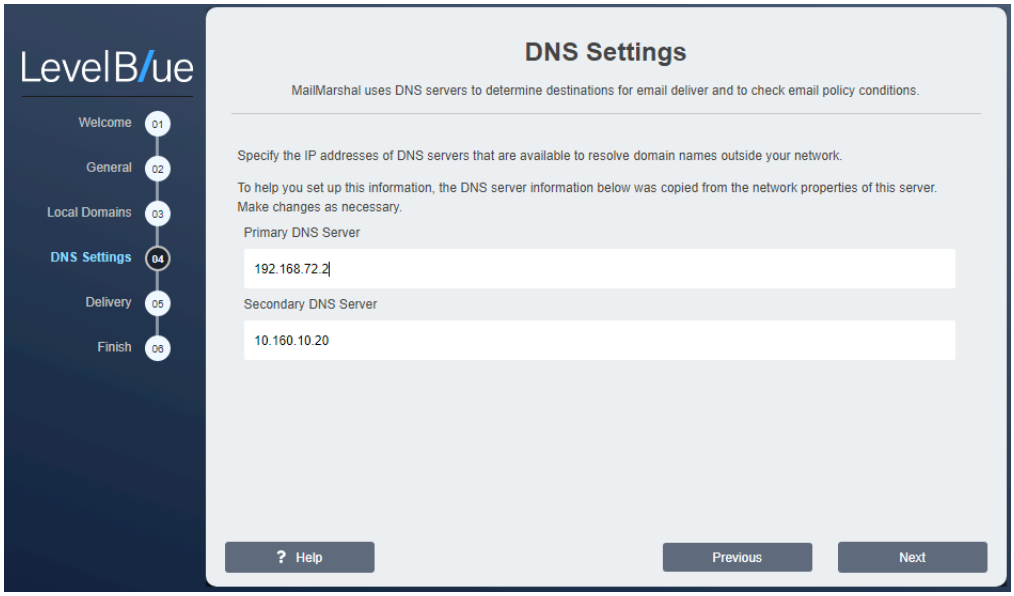
8. On the DNS Settings window, enter the addresses of servers MailMarshal uses for domain name resolution. The wizard pre-populates the fields using Windows DNS settings, but MailMarshal performs DNS lookups independently of the Windows settings. The DNS servers used by MailMarshal should be located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

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

   a. Enter the IP address of the primary DNS server. You must enter a valid IPv4 or IPv6 address.

   b. Enter a secondary address. You can leave this entry blank, but your configuration is more robust if you supply a secondary DNS server.

Copyright © 2026 Trustwave Holdings, Inc.



c. Click **Next**.

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

> **Note:** After you complete the wizard, you can configure other delivery options, including POP3 delivery, load balancing, and multiple routes. For more information, see “Configuring Delivery Options” on page 189 and “Customizing Settings for Nodes” on page 196.

a. Enter the server name, fully qualified domain name, IPv4 address, or IPv6 address, and the port of a local server that MailMarshal will use to deliver all incoming email (addressed to local domains).

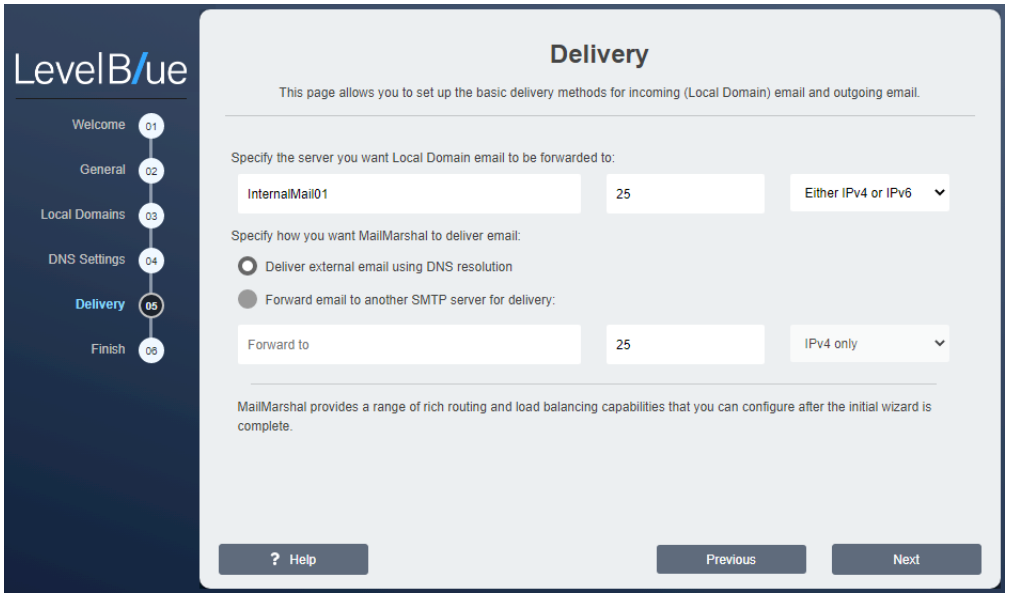
- If you entered a name, you can choose to deliver mail over IPv4, IPv6, or either protocol.

b. Choose to deliver outgoing email directly using DNS lookup, or to forward email to another server for delivery.

c. If you select “forward email to another SMTP server”:

- Specify the server name, fully qualified domain name, IPv4 address, or IPv6 address, and the port of the server (usually port 25). For instance, use this option to send all outbound email through the email servers at your ISP.
- If you entered a name, you can choose to deliver mail over IPv4, IPv6, or either protocol.

Copyright © 2026 Trustwave Holdings, Inc.



d. Click **Next**.

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

When you complete the Configuration Wizard, MailMarshal starts the email processing services and opens the main Management Console page. Use the Management Console to perform additional configuration tasks. You will need to complete some tasks to implement minimum best practices for MailMarshal installation and email filtering. For more information, see “Configuring Email Routing” on page 52, “Configuring Antivirus Scanning” on page 54, and “Configuring Antivirus Scanning” on page 54.

3.6 Configuring Email Routing

After you install MailMarshal and run the Configuration Wizard, you may need to change the email routing on other computers so the MailMarshal Server becomes the gateway for incoming and outgoing email. For more information, see “Understanding Installation Scenarios” on page 24. These routing changes can require you to adjust one or more of the following items:

DNS MX records

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

Internal email server settings

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

Copyright © 2026 Trustwave Holdings, Inc.

Port settings

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

Firewall or relay server settings

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

3.7 Creating Directory Connectors

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

To create a directory connector:

1. Open the MailMarshal Management Interface website.
2. In the left menu, expand **Policy Elements**.
3. In the right pane, click **Connectors.**
4. Click **Add.**



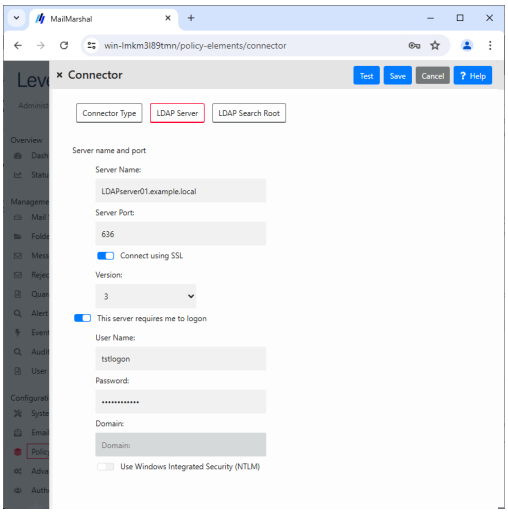
Note: For detailed guidance on fields, click Help.

5. On the Connector Type tab, choose the type of directory this connector will access. MailMarshal supports connections to Azure Entra, Microsoft Active Directory and several types of LDAP directories.
6. Enter a connector name and description
7. In the Reload Schedule section, specify how often MailMarshal will import directory information through this connector, and then click **Next.**
8. *If this is an Azure Entra connection,* on the Entra Properties tab, enter the required credentials. For more details about generating and retrieving the credentials from Entra, see LevelBlue Knowledgebase article Q21246.
9. *If this is a Microsoft Active Directory connection,* on the Microsoft Active Directory Logon tab, choose to connect as anonymous, or as a specific account. If you choose to connect using a specific account, enter the account details.
10. *If this is an LDAP connection,* specify the following information:

Copyright © 2026 Trustwave Holdings, Inc.

a. Select a specific type of LDAP directory server from the list. MailMarshal sets default parameters to retrieve group and member details for the type of server you choose.

b. On the LDAP Server tab enter the server name, port, and logon information if required. If you choose to log on using a specific account, specify the account details. If you do not know the required information, contact the administrator of the LDAP server.



c. On the LDAP Search Root tab, identify a search root for this server. If you do not know whether a search root is required, contact the administrator of the LDAP server.

d. *If this is a generic LDAP connection,* on the LDAP Group Attributes and LDAP User Attributes tabs, customize the information MailMarshal will use to query the LDAP server for group names and group members. For details of the fields, see Help.

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

11. Click **Test** to validate the connection settings. Click **Save** to create the connector.

The properties of an LDAP connector include advanced configuration options that allow you to control which email addresses and groups MailMarshal retrieves. For more information about editing connectors and advanced LDAP configuration, see “Configuring Connectors” on page 126.

3.8 Configuring Antivirus Scanning

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

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

Copyright © 2026 Trustwave Holdings, Inc.

3.8.1 Excluding Working Folders From Virus Scanning

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

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

Some scanners also automatically enable an Internet protection feature. In this case, disable the Internet protection option in addition to disabling the on-access scanning option.

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

If the check succeeds, MailMarshal deletes copies of the `eicar.com` file, preserving the original in the `Unpacking\avcheck` folder.

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

You can verify the location of these folders by running the MailMarshal Server Tool from the MailMarshal Tools group in the MailMarshal program group on each Server. Click the Folders tab to see the folder locations. For more information, see “Changing Folder Locations” on page 205.

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

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

```
C:\Program Files\Trustwave\Secure Email Gateway\Quarantine

C:\Program Files\Trustwave\Secure Email Gateway\Queues\Decryption

C:\Program Files\Trustwave\Secure Email Gateway\Queues\Incoming

C:\Program Files\Trustwave\Secure Email Gateway\Unpacking
```

MailMarshal uses folders in the `Quarantine` folder to store messages, including those quarantined by virus scanning rule actions. The product stores email in the `Queues\Decryption` and `Queues\Incoming` folders pending processing.

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

Copyright © 2026 Trustwave Holdings, Inc.

3.8.2 Configuring MailMarshal to Use an Antivirus Product

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

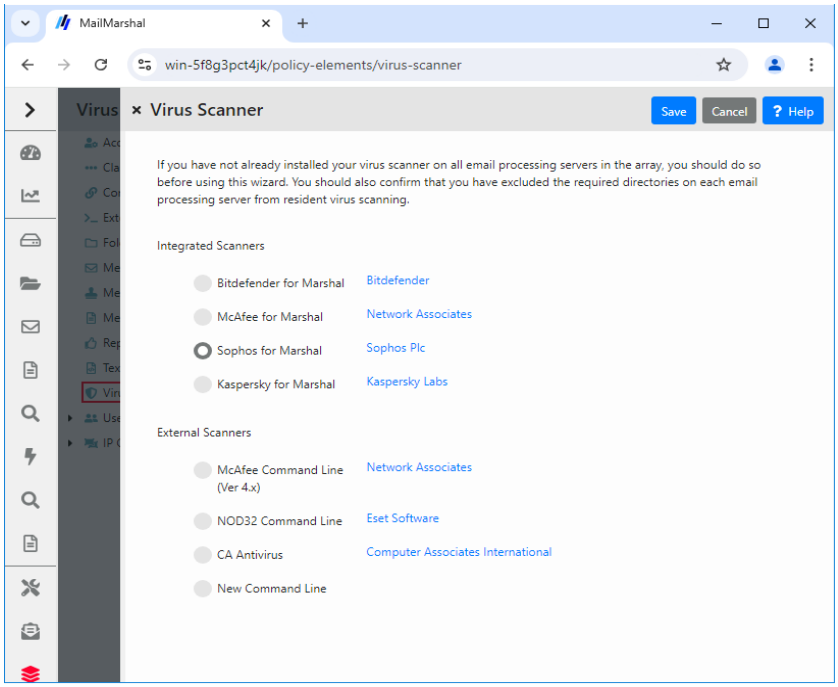
If you install command line virus software on more than one MailMarshal Server, you must install it in the same location (same drive letter and folder) on each Server.

To configure virus scanning in MailMarshal:

1. Ensure you have installed one or more supported virus scanners on each MailMarshal Server computer, following the manufacturer's instructions.
2. Ensure the scanner does not perform on-demand scanning of the MailMarshal excluded folders. For more information, see “Excluding Working Folders From Virus Scanning” on page 55.
3. Access the MailMarshal Management Console website.
4. In the left pane, under **Configuration**, expand **Policy Elements**.
5. In the right pane menu list, click **Virus Scanners.**
6. In the left pane of the Management Console, click **Policy Elements**, and then select **Virus Scanners.**
7. Click **Add**.

Note: For detailed guidance on adding scanners, click Help.

8. Select your antivirus scanner from the list.



Copyright © 2026 Trustwave Holdings, Inc.

9. *If you are configuring a command line scanner,* in the Path field, enter the location of the antivirus scanner program, such as `c:\McAfee\Scan.exe`.
10. *If your command line scanner is not in the list and you selected* ***New Command Line***, specify the additional details required. For assistance see Help.
11. Click **Save** to add the virus scanner. MailMarshal will test the action of the scanner on each installed MailMarshal email processing server.
12. *If you plan to use more than one virus scanner,* repeat Steps **7** through **11** for each scanner.

3.9 Installing and Customizing Web Components

In addition to the web Management Console, MailMarshal includes a Spam Quarantine Management console that allows email recipients to review and manage their own quarantined messages.



Caution: As best practice for security, do not install these components on a server exposed to the Internet. For more information, see Knowledgebase article Q21022.

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

For more information about hardware and software requirements, see “Web Components Requirements” on page 34.

3.9.1 Installing the MailMarshal Web Components

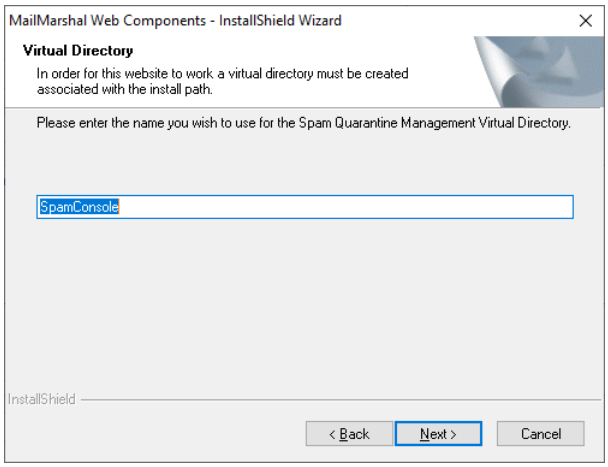
Run the Web Components setup to install the MailMarshal Spam Quarantine Management (SQM) Website.

To install the SQM website:

1. Ensure you have installed all prerequisite software specified for a Web components computer, and opened required ports for communication with the Array Manager and client browsers. For more information, see “Web Components Requirements” on page 34.
2. Log on as a local administrator to the computer on which you want to install the MailMarshal Web components.
3. Close any open applications.
4. Run the setup program from the MailMarshal installation kit.
5. On the Setup tab, click **Web Components Setup**.
6. On the Welcome window, click **Next.**
7. On the License Agreement window, carefully read the license information.
8. Click **I accept the terms of the license agreement,** and then click **Next.**
9. Choose a destination location and program folder. Web Components install as a 32 bit application. By default the location is `C:\Program Files (x86)\Trustwave\SEG Web Components`.

Copyright © 2026 Trustwave Holdings, Inc.

10. On the Virtual Directory window, enter a website directory name. This name becomes the virtual path of the site URL, in the default website on the server.

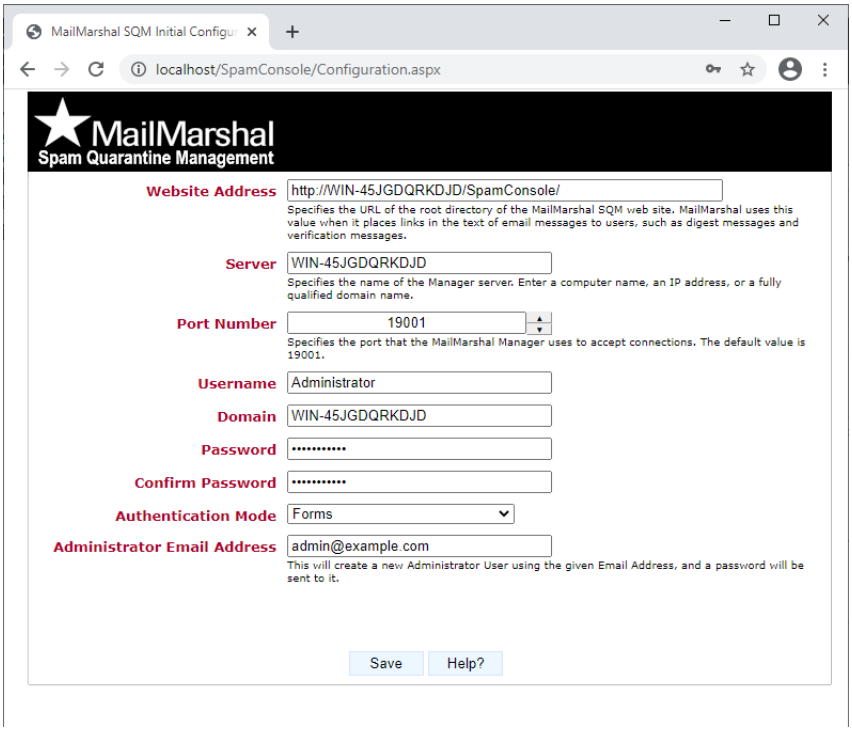


11. Click **Next.**
12. On the Ready to Install the Program window, click **Install**.
13. On the Setup Wizard Complete window, click **Finish.**
14. To complete setup of the Spam Quarantine Management website, open a supported web browser. The default URL for this site is `http://IISServerName/SpamConsole` where *`IISServerName`* is the name of the Microsoft IIS server where you installed the Web components.
15. On the configuration page of the Spam Quarantine management site, specify the Site URL, Array Manager connection information, User Authentication method, and User Interface settings. For more information, click **Help**.

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

Copyright © 2026 Trustwave Holdings, Inc.

Figure 6: Spam Quarantine Management configuration page



16. As part of Spam Quarantine management site setup, the site creates an administrator login (for the specified email address, or the Windows login used to access the configuration page). You can change many site settings later by logging in to the site using the Administrator login.

3.9.2 Customizing the Web Components

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

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

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

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

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

Copyright © 2026 Trustwave Holdings, Inc.

3.10 Upgrading MailMarshal

MailMarshal 12.0 supports upgrade from version 10.1.0 and above.



Note: If you plan to use a new server for the new version and you want to keep existing configuration, you must still upgrade.

3.10.1 Upgrading from MailMarshal Version 10.1.0 or Above

You can upgrade directly to the latest release of MailMarshal from these versions. Upgrade the Array Manager first. Then upgrade other MailMarshal components



Note: To upgrade from earlier versions, first upgrade to a version that supports direct upgrade. You should also consider a clean installation of the current version.

To upgrade to the latest version of MailMarshal:

1. Ensure the computer you want to upgrade meets the prerequisites for the latest version of MailMarshal.
   - You must enable the Windows Authentication feature in IIS.
2. Ensure the Microsoft SQL Server is a supported version. For supported direct upgrades, no change in SQL Server is required.
3. Log on as a local administrator to the MailMarshal Array Manager computer.
4. Verify anti-virus exclusions.
5. Back up your MailMarshal configuration. Use the MailMarshal 10.X Management Console. You can also use the `MMExportCfg` command line tool.
6. Close any running MailMarshal user interfaces (including Server Tool, other tools, and web interfaces).
7. Run the MailMarshal setup program from the installation package.
8. On the Setup tab, click **Install MailMarshal.** On the Welcome window, the setup program displays the current version of MailMarshal and the version to which it will upgrade. Click **Next**.
9. On the License Agreement window, carefully read the license information.
10. Click **I accept the terms of the license agreement,** and then click **Next.**
11. On the Ready to Install window, click **Install**.
12. The setup program stops the MailMarshal services, installs any required prerequisites, updates the product files and database, installs the management websites if required, and starts the services.
13. On the Update Complete window, click **Finish**.
14. If you are upgrading a MailMarshal Array, install the software on each processing server.
15. Open the Management Console website, verify that each email server is connected and to ensure the Receiver, Engine, and Sender services are running.
16. If you are using the MailMarshal Web components:

Copyright © 2026 Trustwave Holdings, Inc.

a. *If you have customized any Web component graphics*, make a backup copy of the custom files to a backup folder. For more information, see “Customizing the Web Components” on page 59.

b. On the Web components computer, run the MailMarshal setup program from the installation package.

c. On the Setup tab, click **Install Web Components**.

d. Run the Web components setup until you have completed the installation process. If the previous version of the Admin Console website was installed it will be removed.

e. *If you backed up custom graphic files*, copy your backup files to the proper locations in the new install folders.

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

3.10.2 Upgrading from Other Versions of MailMarshal

To upgrade from a MailMarshal version prior to 10.1.0, *except 8.3.2*, first upgrade to 10.1.0. For version 8.3.2, first upgrade to 10.2.5.

See the release notes for each version, available on the “previous versions” page of the LevelBlue website.



Tip: Instead of upgrading from a version 8.X installation, consider a clean installation. Clean installation helps to ensure that all new features are used. Clean installation also makes it easier to review and eliminate outdated policy exceptions and deprecated policies.

There are several important steps to the upgrade process. Review the available documentation before beginning.

3.11 Uninstalling MailMarshal

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

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

To uninstall MailMarshal:

1. Connect to the MailMarshal Management Console.
2. In the left pane, select **Mail Servers**.
3. In the right section of the right pane, select the Server you wish to uninstall and then click **Edit**.
4. On the **General** tab, **Services** section, select the **Receiver** service, and then click **Stop**.
5. Allow the Engine and Sender services to run until MailMarshal processes all the received email. You can verify that all mail queues are empty by viewing the lists in the menu tree of the main **Mail Servers** page.

Copyright © 2026 Trustwave Holdings, Inc.

6. Reroute your email delivery settings to exclude the MailMarshal Server you want to uninstall. For example, you may need to change the DNS MX records, firewall translation settings, and internal email server settings that directed email to the MailMarshal server both from external email and from your internal email server.
7. Verify that email is flowing through the new path and no email is being delivered to the MailMarshal server you plan to uninstall.
8. *If you want to preserve the data from the MailMarshal Server you are uninstalling, b*ack up the contents of the MailMarshal `Quarantine` folder and all sub folders.
9. On the server you want to uninstall, run Add/Remove Programs in Control Panel to remove MailMarshal. You may have to restart your computer to remove some program files.
10. To delete the `Quarantine` folders, first delete the contents of the `Symbolic` sub folder.
11. Delete the remaining `Quarantine` folders and files.
12. If you are using a MailMarshal array and want to remove the product completely, repeat Steps 1 through 12 on each additional email processing server.
13. Use Add/Remove Programs from the Windows Control Panel to remove additional components you may have installed, such as Web Components.
14. Use Add/Remove programs from the Windows Control Panel to remove the MailMarshal Array Manager. The Management Console will also be removed.

Copyright © 2026 Trustwave Holdings, Inc.

4 Understanding MailMarshal Interfaces

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

MailMarshal Management Console Website

Allows you to:

- Manage and customize your content security policy, and configure email delivery options.
- Monitor server health and email traffic flow on a real-time basis, manage quarantined email messages, and audit actions on quarantined messages.
- Set up delegated quarantine management with email digests and the SQM website.

MailMarshal Spam Quarantine Management Website

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

Other Tools

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

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

4.1 Understanding the MailMarshal Web User Interface

The MailMarshal Management Console User Interface (Management Console) combines the policy management and email management functions of the legacy MMC Configurator and Console. The Management Console is always installed on a standalone MailMarshal server, or on the Array Manager server when you install a MailMarshal array.



Caution: As best practice for security, do not install the Management Console on a server exposed to the Internet. For more information, see Knowledgebase article Q21022.

Multiple users can connect to the Management Console from any location that can access the site.



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

Copyright © 2026 Trustwave Holdings, Inc.

The left pane of the Management Console shows the main menu. The right pane of the Management Console shows details of the item selected in the main menu. In some cases the detail view includes another menu tree or other navigation features to organize the information provided (such as the policy view). Additional details may open in pop-up windows or additional panels.

Note: Many items in the Management Console include a right-click menu that lets you choose context-sensitive actions.

To start the Management Console, open a supported web browser and navigate to the default website of the Array Manager server.

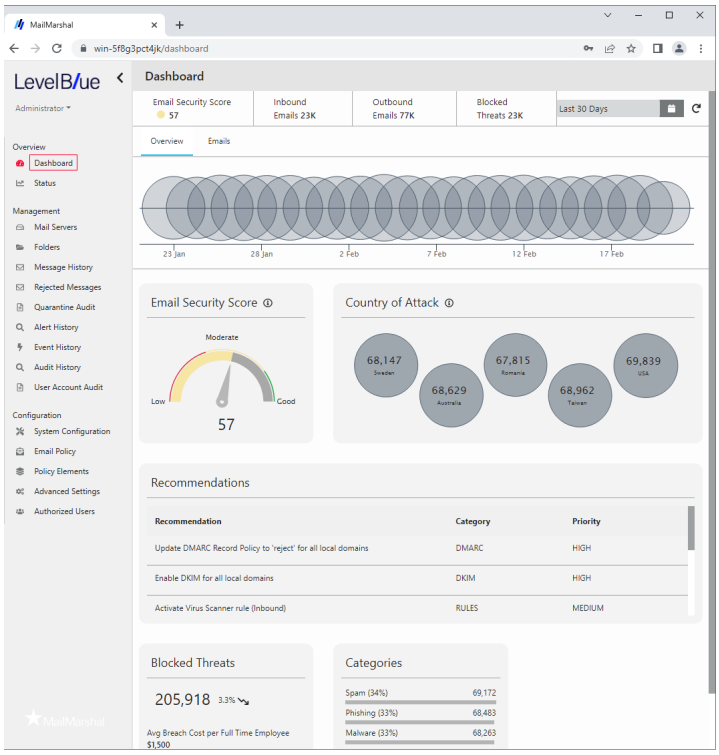
4.1.1 Working With the Dashboard and Status pages

When you start the Management Console, you must log in using the default credentials or credentials you created.

Caution: As best practice for security, immediately change the default password and/or create additional accounts. See the menu item **Authorized Users)**.

In the default view, the right pane shows a dashboard giving details of email security protection activity, as well as an evaluation of the security configuration.

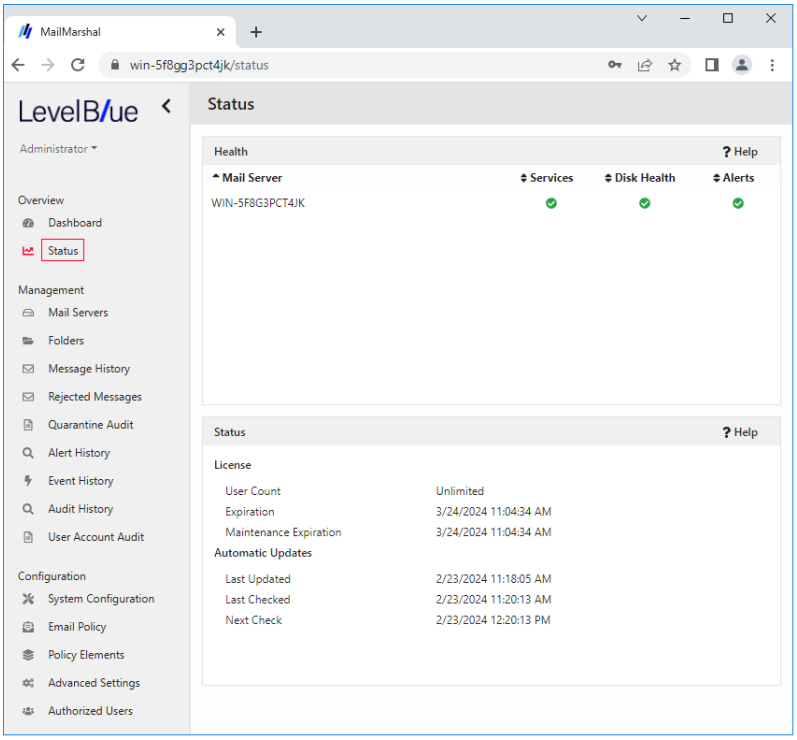
Figure 7: Management Console Dashboard



The next menu selection is the Status page. This page shows information about server health at a glance.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 8: Management Console Status



4.1.2 Working With Menu and Detail Items

View the details for a menu item by clicking the item. Some items such as Policy Elements open an additional menu. Expand the menu by clicking the arrow to the left of a heading.

View detailed properties of an item by selecting it.

Some menu items such as policy elements include a list. To see details of an item in the list, double-click it.

4.1.3 Working With Properties Configuration

You can set many global properties of MailMarshal using two properties items.

System Configuration

This item allows you to configure basic properties of the MailMarshal installation. You can control how MailMarshal receives and delivers email and you can also set up some email filtering that will be applied to all messages. To open this item, from the main menu select **System Configuration**. To view and change specific settings, select an item from the menu tree at the left of the Properties panel.

Node Properties

Each MailMarshal installation includes one or more email processing servers, also known as nodes. To see a list of these servers, from the main menu select **Mail Servers**. The right pane dis-

Copyright © 2026 Trustwave Holdings, Inc.

plays a list of installed servers. To configure settings for a server, double-click to select that server in the list, then use the tab buttons to review specific settings. To review mail processing service activity, expand the tree on the left of the panel.

For more information about the properties and settings shown on these windows, see “Configuring Email Content Security” on page 70 and “Managing Array Nodes” on page 195

4.1.4 Committing Configuration

Changes you make to the MailMarshal configuration are not applied to email processing servers immediately. If configuration has not been committed, the top right of the Management Console shows a button **Commit Pending Changes**. To review and apply the changes, click the button.

If you have configured “commit scheduling,” then committing configuration might not apply the configuration to the email processing servers immediately. For more information about commit scheduling, see Help for **Advanced System Properties > Commit Scheduling**.

4.1.5 Change Auditing

MailMarshal keeps a history of changes to configuration. You can audit changes in detail.

To see the full list of changes:

1. In the left pane menu click **Audit History**.
2. On the Audit History screen, drill down to an individual change (commit) set, or an individual item.

To see changes to an individual item:

1. In the left pane menu select **Email Policy** or **Policy Elements**.
2. Select a policy or element type to see a list of items.
3. Select an item and then click **Audit**. You can view more details, or revert the change.



Note: Reverting adds a change to the pending changes. You must commit configuration to apply the change.

4.1.6 Managing Authorized Users

MailMarshal enforces access to the Console and API with authorized user accounts, Windows credentials, or Single Sign On using SAML.



Tip: New installations use the MailMarshal user accounts by default. Upgrades from MailMarshal 8.X use Windows Authentication by default and attempt to maintain access levels set in the earlier version. To change the authentication method, use the Config Service Admin Tool (see “Using the Config Service Admin Tool” on page 209).

A user can have one or more of the following roles:

- **Superuser:** Has full control over logins and all aspects of the console.
- **Admin:** Has access to the configuration sections of the console, but not logins or security.
- **Helpdesk:** Has access only to the email management sections of the console.

Copyright © 2026 Trustwave Holdings, Inc.

A new installation creates a Superuser account named `Admin`.

To manage access, in the left pane menu click **Authorized Users**. For full details, see Help.

You can also manage Superusers from the **Users** page of the Config Service Admin Tool.

You can set access to MailMarshal Folders for each role or user. See “Working with Folders” on page 155.

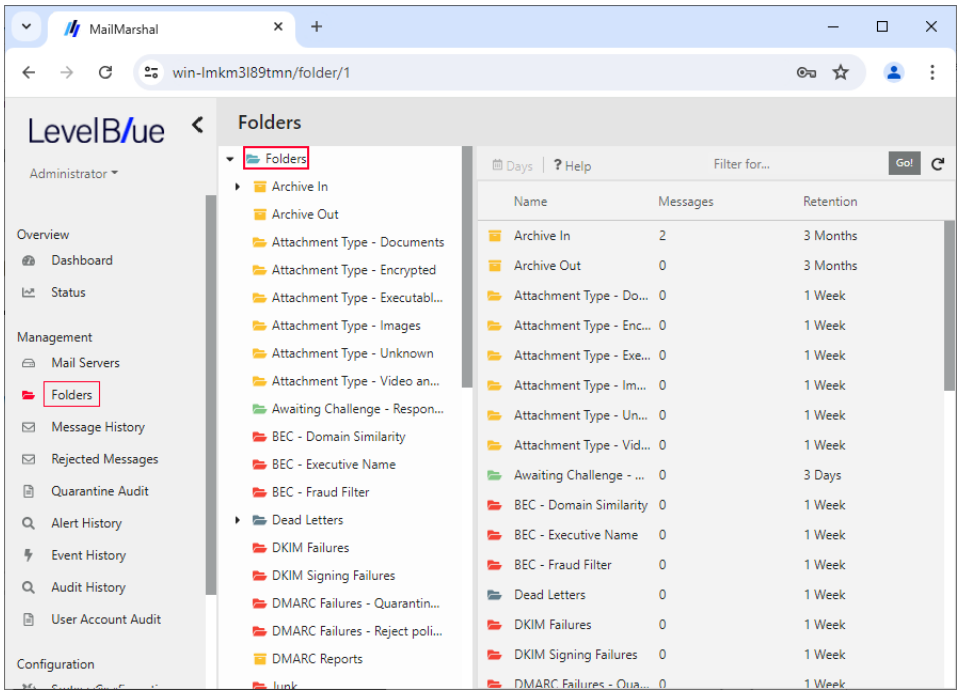
To review changes to Authorized Users, in the left pane menu click **User Account Audit**. Actions audited include addition, deletion, block/unblock, password reset, and changes to name, address, and assigned roles.

4.1.7 Understanding Email Management

Email management in MailMarshal is through the Management section of the Management Console. Important items in this section include:

- **Mail Servers:** review the current service activity on each server, and manage sending queues
- **Folders:** review quarantined or locally stored messages.
- **Message History:** review processing results for all messages including quarantined and delivered messages.
- **Rejected Messages:** review details of connection attempts rejected due to server policy or Connection Rule action.

Figure 9: Management Console Folders



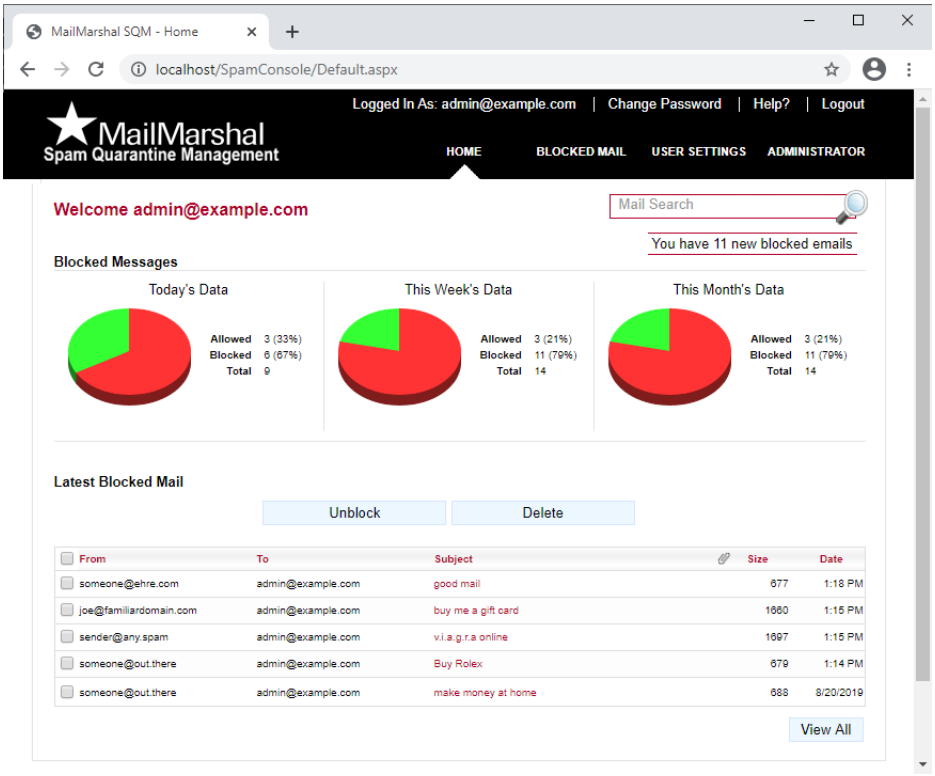
For more information about the features and functions of the Console, see “Using the MailMarshal Console for Email Management” on page 167.

Copyright © 2026 Trustwave Holdings, Inc.

4.2 Understanding the Spam Quarantine Management Website

The MailMarshal Spam Quarantine Management Website (Spam Console) uses Microsoft IIS. The Spam Console can be installed on any Microsoft IIS server that can connect to the MailMarshal server or Array Manager. Spam Console generally works with current versions of major browsers such as Microsoft Edge, Chrome, Firefox, and Safari. The browser must be configured to use JavaScript and to accept cookies. The Spam Console allows users to see a summary of blocked mail, release messages, and manage a variety of settings.

Figure 10: Spam Quarantine Management website



4.3 Understanding Other Tools

The **MailMarshal Server Tool** allows you to change various settings related to folder locations and communication between the MailMarshal components. These settings cannot be changed from within other interfaces for technical reasons. For more information, see Help for this tool.

The settings include:

- Array Manager database connection details
- Array Manager ports for communication with Node (processing) servers
- Array Manager REST service settings
- Credential used to join a node to the array

Copyright © 2026 Trustwave Holdings, Inc.

- Syslog Database connection details (for the optional Syslog integration)
- Node ports for communication with the Array Manager
- Folder locations for Nodes and Array Manager

The **Config Service Admin Tool** allows you to set up the website and database used by the Management Console, and modify Management Console user permissions. For more information, see “Using the Config Service Admin Tool” on page 209.

The **Group File Import Tool** allows you to import user and group information into MailMarshal user groups from a text file. For more information, see “Using the Group File Import Tool” on page 205.

Copyright © 2026 Trustwave Holdings, Inc.

5 Implementing Your Email Content Security Policy

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

An Email Content Security policy typically has several goals:

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

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

5.1 Configuring Email Content Security

Configure email content security using the MailMarshal Management Console. For basic information about the Management Console see “Understanding the MailMarshal Web User Interface” on page 63

Content Security policies generally include elements of two types:

Email transport policies

These policies are implemented using global settings you configure in **MailMarshal Properties**. These policies control who is allowed to send email to or through the MailMarshal server. For more information on email transport policies, see “Configuring SpamProfiler” on page 72, “Preventing Relaying” on page 77 and “Controlling Who Can Send Email Through Your Server” on page 78.

Email content policies

These policies are implemented using rules you configure as part of MailMarshal Email Policy. These policies control the content of email messages. For more information on email content policies, see “Stopping Spam” on page 71, “Stopping Viruses and Malware” on page 75, and “Filtering Messages and Attachments” on page 86.

To start the Management Console, open a supported web browser and navigate to the default HTTPS website of the Array Manager server.

Copyright © 2026 Trustwave Holdings, Inc.

5.2 Stopping Spam

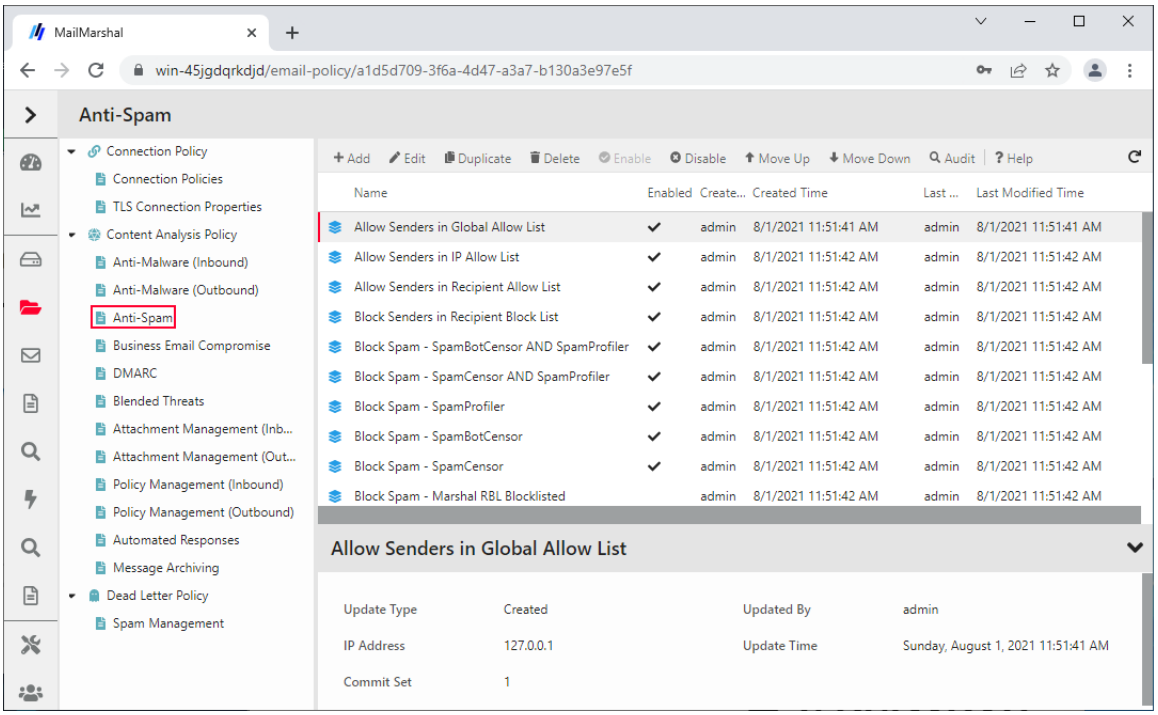
Stopping unsolicited incoming email (commonly known as spam) is a primary goal for most organizations. The LevelBlue SpamCensor and SpamBotCensor technology filter spam efficiently with minimal overhead. The SpamProfiler is a signature based check performed at the Receiver, that allows MailMarshal to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

5.2.1 Anti-Spam Configuration and Rules

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

To view the Spam policy group:

1. In the left pane of the Management Console, expand the item **Email Policy**.
2. In the right pane, **expand Content Analysis Policy** and select **Anti-Spam**.



3. To view details of each rule, including a description of its intended use, select the rule and click **Edit** in the toolbar.

Tip: To see a list of all conditions and actions in a rule, enable **Preview** using the toggle at top right of the rule panel.

Copyright © 2026 Trustwave Holdings, Inc.

The default rules include:

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

  Note: To ensure the reliability of SpamCensor and SpamProfiler, verify that they are enabled and correctly configured. See “Configuring SpamProfiler” on page 72 and “Configuring SpamCensor, SpamProfiler, and YAE Updates” on page 73.

  To ensure the reliability of SpamBotCensor, ensure the processing nodes receive connections directly from the Internet.

- A rule to allow email messages from specific addresses.
- Rules to implement lists of blocked senders and safe senders for each user. Users can update these lists through the MailMarshal Spam Quarantine Management Website.
- A rule to quarantine email messages that contain text relating to scams, using the MailMarshal TextCensor.
- A rule to block spam email that contains spam-linked URLs in the message header or body. The rule uses the URLCensor function to compare URLs in received messages with listings maintained by external blocklist sites. URLCensor decodes URLs intentionally obscured with decimal, octal, or hexadecimal notation. For more information about using URLCensor, see the LevelBlue Knowledgebase.

  Note: To use URLCensor, you must ensure that MailMarshal uses a reliable, efficient DNS server. For more information, see “Configuring Default Delivery Options” on page 189.

5.2.2 Configuring SpamProfiler

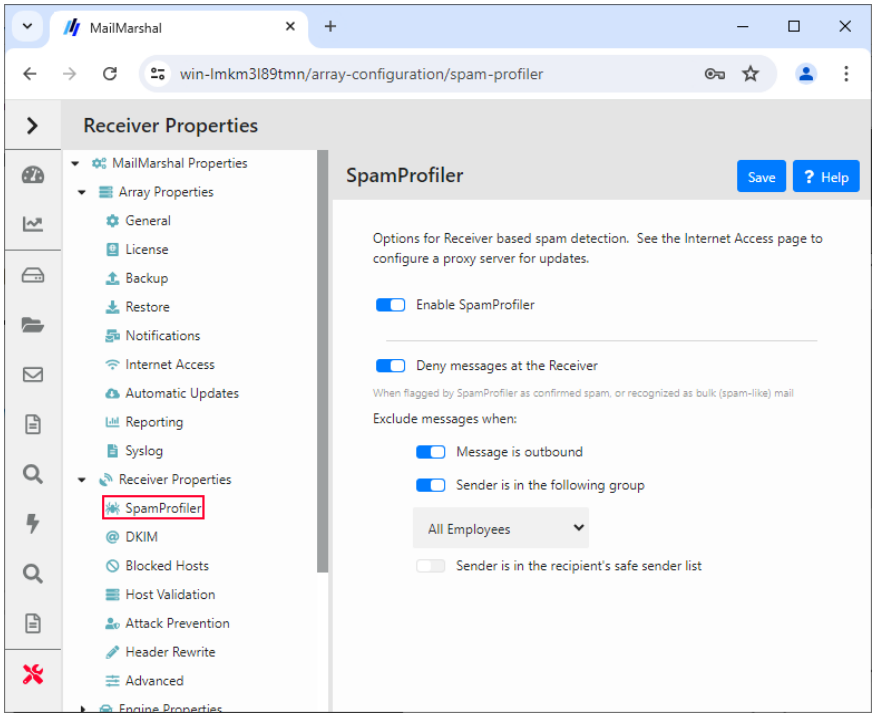
SpamProfiler is a signature based service that examines email at the MailMarshal Receiver. SpamProfiler can significantly reduce the load on the MailMarshal Engine. By default MailMarshal enables SpamProfiler and uses Content Analysis Policy rules to quarantine messages in a folder. You can also use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

To configure SpamProfiler:

1. In the Management Console, select **System Configuration** and then expand **Receiver Properties**.
2. To enable **SpamProfiler**, select it from the menu and select **Enable SpamProfiler.**
3. To block message at the receiver, select the option **Deny messages**. You can exclude groups of senders from blocking using the additional options. For details of the options, see Help.

   Tip: A message is blocked at the Receiver if SpamProfiler classifies it as confirmed spam. To take action on other messages that SpamProfiler classifies, use the Content Analysis Policy rule condition **Where message is detected as spam by SpamEngine.**

Copyright © 2026 Trustwave Holdings, Inc.



4. To quarantine or delete messages, enable SpamProfiler and then use the Content Analysis Policy rule condition **Where message is detected as spam by SpamEngine**. For more information see “Where message is/is not detected as spam by SpamEngine” on page 95.

Tip: When SpamProfiler is used with Content Analysis rules (not blocking at the Receiver), some suspect messages may be held briefly for rescan. Rescanning helps to improve the accuracy of SpamProfiler detection. Rescanning does not significantly delay processing.

5.2.3 Configuring SpamCensor, SpamProfiler, and YAE Updates

LevelBlue provides updates for the SpamCensor, SpamProfiler, and Yara Analysis Engine (YAE) facilities to all customers with current MailMarshal maintenance contracts. The updates are delivered through the Web by HTTP and HTTPS.

Tip: To check the maintenance entitlement for this installation, see the Maintenance Expiry section on the License page (**System Configuration > License).**

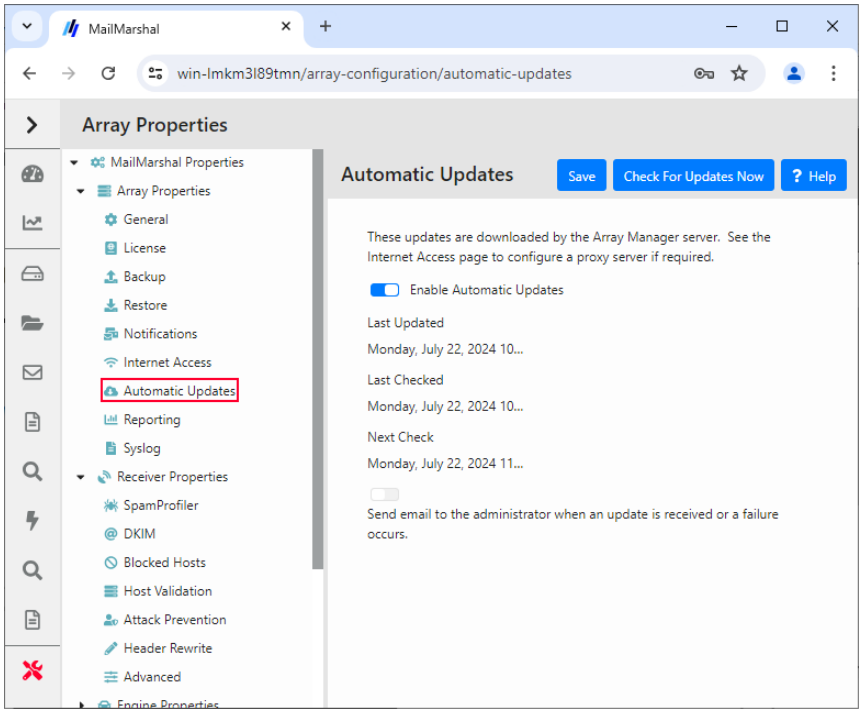
5.2.3.1 Configuring and Checking Automatic SpamCensor Updates

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

To monitor and configure SpamCensor updates:

1. In the Management Console, select **System Configuration** and then expand **Array Properties.**
2. Select **Automatic Updates** from the menu. The display shows the time and result of the last update attempt, and the time of the next attempt.

Copyright © 2026 Trustwave Holdings, Inc.



3. *If you do not want the SpamCensor to update automatically,* toggle off **Enable Automatic Updates.**
4. *If you want to be notified by email when a SpamCensor update is received or a problem occurs,* toggle on **Send email to the administrator.** MailMarshal sends an email message to the administrator address configured on the Notifications page of MailMarshal Properties.
5. *If you want to perform a check for SpamCensor updates immediately,* click **Check for Updates Now.**

5.2.3.2 Configuring Proxy Settings for Updates

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

SpamCensor updates are downloaded by the Array Manager. SpamProfiler updates are downloaded by each processing node.

To configure proxy settings for the updates:

1. In the Management Console, select **System Configuration** and then expand **Array Properties.**
2. Select **Internet Access** from the menu.
3. You can configure the following settings for the Array Manager (SpamCensor updates) and for the *processing nodes (SpamProfiler updates).*
   a. *If you want MailMarshal to access the Web directly,* select **Direct Access.**
   b. *If you want MailMarshal to use a specific proxy server,* select **Proxy.** Enter a proxy server name and port. If necessary, enter a user name and password for proxy authentication.

Copyright © 2026 Trustwave Holdings, Inc.

4. To apply the proxy settings, click **Save** and then commit MailMarshal configuration changes.

You can also configure different proxy settings for each processing node if necessary. For more information, see “Customizing Settings for Nodes” on page 196.

5.3 Stopping Viruses and Malware

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

MailMarshal also provides additional important layers of protection against malware using proprietary Zero Day updates, Yara Analysis Engine malware detection, and the Outbreak Detection function of SpamProfiler.

5.3.1 How MailMarshal Uses Virus Scanners

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



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

For more information about configuring virus scanners, see “Configuring Antivirus Scanning” on page 54.

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

5.3.1.1 Features

MailMarshal supports the following virus prevention and management features:

- Email antivirus scanning at the gateway: Adds a proactive layer of defense at a key strategic point in the network.
- **Multiple virus and malware scanners (optional):** Increases the chances of detecting a virus and reduces the vulnerabilities from delays in patch updates.
- **Virus notification and reporting:** Provides email notifications of specific viruses, and comprehensive reporting on virus incidents (including the virus names if provided by the scanner in use).

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

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

Copyright © 2026 Trustwave Holdings, Inc.

5.3.1.2 Implementation Options

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



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

Install one or more chosen scanners on each MailMarshal email processing server following the manufacturer's instructions. For more information about supported antivirus software, see “Supported Antivirus Software” on page 37. For more information about installing virus scanners, see “Configuring Antivirus Scanning” on page 54.



Tip: Several integrated scanners are available through LevelBlue, including implementations of Bitdefender, McAfee, and Sophos. These software packages are available from links in the MailMarshal installation package, or in separate downloads from LevelBlue.com.

5.3.2 Anti-Malware Policy and Rules

The default email policy provided with MailMarshal includes two policy groups titled Anti-Malware (Inbound) and Anti-Malware (Outbound). These policy groups include a number of rules to block viruses and malware.

To view the Anti-Malware policy groups:

1. In the left pane of the Management Console, select the item **Email Policy**.
2. Expand **Content Analysis Policy**, and select the item **Anti-Malware (Inbound)** or **Anti-Malware (Outbound).**
3. To view details of each rule, including a description of its intended use, double-click the rule name in the right pane.

The default rules include rules to implement Zero Day protection and Yara Analysis Engine action, to attempt to block malware infected email messages using traditional scanners, to block malware-related messages by their content, and to apply SpamProfiler's Outbreak Detection technology.

The rules that invoke malware scanners are disabled by default. You must install and configure at least one scanner before you can enable these rules.

5.3.3 Best Practices

LevelBlue recommends the following basic practices to ensure security with respect to malware/viruses and scanning:

- Ensure that SpamCensor and SpamProfiler updating is enabled, to provide a Zero Day layer of protection. The SpamCensor updater also delivers updates for the Yara Analysis Engine and file unpacking.
- Block messages and attachments that MailMarshal cannot scan, such as password protected attachments and encrypted attachments (for example files of type ‘Encrypted Word Document’).

Copyright © 2026 Trustwave Holdings, Inc.

- Block encrypted messages that MailMarshal cannot decrypt, such as PGP and S/MIME messages and encrypted ZIP files.
- Block executable and script files by type and name. This helps to ensure that unknown viruses will not be passed through.
- Subscribe to email notification lists for malware outbreaks. Such lists are available from many antivirus software companies. When an outbreak occurs, block the offending messages by subject line or other identifying features.



Note: If resident or "on access" virus scanning is enabled, exclude the MailMarshal working folders from scanning. See "Excluding Working Folders From Virus Scanning" on page 55. Some integrated scanners use additional temporary locations, and these must also be excluded. See release notes for the specific scanners.

5.3.4 Viewing Virus Scanner Properties

Double click the name of any virus scanner in the right pane to review MailMarshal configuration information for that scanner. With external scanners you can modify the configuration. For details of the fields, see the Help for this panel.

5.4 Preventing Relaying

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

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

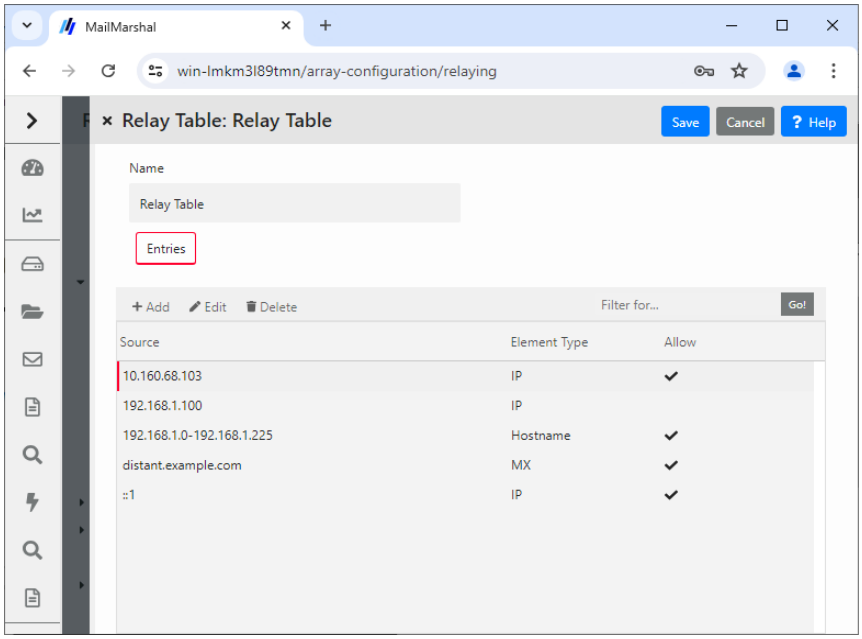
You may need to allow relaying from other locations. You can allow relaying in two ways:

- By specific account authentication. See "Authentication by Account" on page 81.
- By Relaying Table.

To permit relaying from other locations:

1. In the Management Console, select **System Configuration** and then select **Relaying**.
2. In the right pane, double-click the default Relay Table entry. The Relay Table panel displays the list of sources allowed or denied relay permission.
3. To permit relaying from additional computers, click **Add**.
4. In the Relay Table Entry panel select one of the available options, and then enter the required data. You can use a single IPv4 or IPv6 address, a hostname, or a MX lookup for a domain. For example, you can choose to permit relaying from the IP range 10.15.1.0– 10.15.1.255.

Copyright © 2026 Trustwave Holdings, Inc.



5. Click **Save** to both panes, and then commit configuration changes.

Note: For more details of the available options, see “Configuring Relaying” on page 188. For details of the fields on the windows, click Help.

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

5.5 Controlling Who Can Send Email Through Your Server

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

5.5.1 Reputation Services and DNS Blocklists

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

Note: Reputation Services results are based on the IP address of a server, and currently provide information about IPv4 addresses only.

Copyright © 2026 Trustwave Holdings, Inc.

The Marshal IP Reputation Service (provided by LevelBlue) is automatically provisioned. You can configure details of other services in Policy Elements. You can configure one or more Connection Policy or Content Analysis Policy rules to filter email based on the list information.

Tip: Default policy for new installations includes an enabled Connection rule to use the Marshal IP Reputation Service.

5.5.1.1 Recommended Usage

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

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

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

You can also use reputation services in Content Analysis Policy 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 technical reference "MailMarshal Anti-Spam Configuration," available from the LevelBlue website. You can view the result returned by a Category reputation service lookup in the message log (if the message is quarantined) or the MailMarshal Engine text log.

5.5.1.2 Configuring Access to a Reputation Service

MailMarshal maintains a list of available reputation services it can use in Connection Policy rules.

To configure access to a reputation service:

1. In the Management Console, expand **Policy Elements** and select **Reputation Services**. The right pane shows a list of configured services.

   Note: The Marshal IP Reputation Service will be automatically provisioned for use by trial installations and customers with current maintenance.

   Provisioning requires Internet access from the Array Manager server.

2. You can edit or test a service entry or add a new entry. See Help for details of the required information.

5.5.1.3 Using a Reputation Service Rule

The default email policy provided with MailMarshal includes a Connection Policy rule that uses the Marshal IP Reputation Service. This policy is enabled by default.

To disable or re-enable the default Reputation Service rule:

1. Verify that the Marshal IP Reputation Service is present in the list of Reputation Services. This service is enabled by default in current versions of the product.
2. In the left pane, expand the item **Email Policy.**
3. Expand **Connection Policy** and double-click **Connection Policies.**

Copyright © 2026 Trustwave Holdings, Inc.

4. In the right pane, double-click the rule **Deny Trustwave Reputation Service Blocklisted on connection.** On the General tab, toggle the **Enabled** status, and then click **Save**.
5. Commit the configuration changes.

5.5.2 PTR Lookups

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



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

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

To edit the PTR lookup policy:

1. In the Management Console, select **System Configuration** and then expand **Receiver Properties.**
2. Select **Host Validation** from the right pane menu.
3. To validate hosts sending incoming email using DNS information, toggle on **Validate connecting hosts in the DNS**. MailMarshal will perform a reverse DNS lookup on each IP address from which email is being sent.
4. Select an option using the radio buttons.
   - Choose **Accept unknown hosts** to accept email from hosts without appropriate DNS information, but log this fact to the MailMarshal Receiver text log.
   - Choose **Host must have a PTR record** to block messages from any host that does not have a valid DNS PTR record. Blocked messages are logged in the Windows Event Log and return the SMTP response: `554 No SMTP service here`.
   - Choose **PTR Record must match the HELO connection string** to block messages from hosts whose PTR domain does not match the HELO identification sent by the server. This is the most restrictive option. Blocked messages are logged in the Windows Event Log and return the SMTP response: `554 No SMTP service here`.
5. To implement the blocking, click **Save** and then commit configuration.

5.5.3 Blocked Hosts

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

To edit the list of Blocked Hosts:

1. In the Management Console, select **System Configuration** and then expand **Receiver Properties**
2. Select **Blocked Hosts** from the right pane menu.

Copyright © 2026 Trustwave Holdings, Inc.

3. Toggle on **Refuse Mail...** and then add server names, IP addresses, or IP address ranges to the list. For information about the format of entries, see Help.
4. To implement the blocking, click **Save** and then commit the configuration.

5.5.4 Authentication by Account

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

To use authentication by account:

1. Create and maintain a list of accounts using the policy element Accounts. For more information see “Setting Up Accounts” on page 191.



Note: You can also check authentication using an Active Directory group. For details of this option, see Knowledgebase article Q16649.

2. Configure MailMarshal to advertise ESMTP authentication. For more information see “MailMarshal Properties – Advanced” on page 200.
3. Create a Connection Policy rule using the condition “Where sender has authenticated”. For information about creating rules see “Understanding Rules” on page 90. For information about this rule condition see “Where sender did/did not authenticate successfully” on page 111.



Note: You can also check the authentication of messages using a Content Analysis Policy rule. For more information, see “Where the DKIM verification result is” on page 109. Using Content Analysis Policy to check authentication provides more flexibility in actions and other conditions, but could reduce security.

5.6 Preventing Malicious Email Attacks

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

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

5.6.1 Understanding Denial of Service Attack Prevention

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

5.6.1.1 How MailMarshal Prevents Attacks

MailMarshal prevents DoS attacks by the following means:

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

Copyright © 2026 Trustwave Holdings, Inc.

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

5.6.1.2 Optimizing DoS Attack Prevention Settings

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

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

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

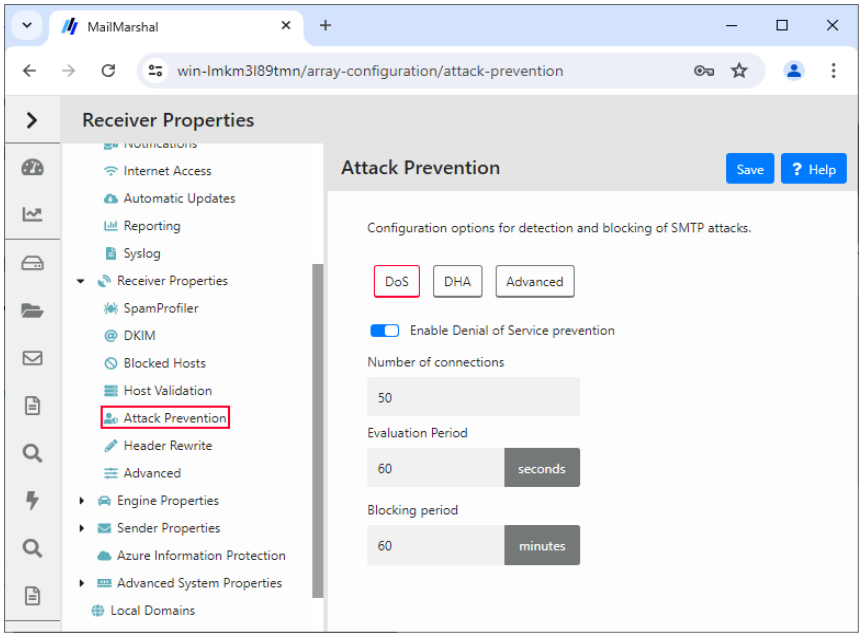
5.6.2 Preventing Denial of Service Attacks

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

To configure DoS attack prevention:

1. In the Management Console, select **System Configuration** and then expand **Receiver Properties.**
2. Select **Attack Prevention** in the right pane menu, and select the **DoS** tab.
3. Select (toggle on) **Enable Denial of Service prevention**, and specify values. For more information about the fields and settings, click **Help**.

Copyright © 2026 Trustwave Holdings, Inc.



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

5.6.3 Enabling and Disabling DoS Attack Prevention

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

To enable or disable DoS attack prevention:

1. In the Management Console, select **System Configuration** and then expand **Receiver Properties**
2. Select **Attack Prevention** in the left pane, and select the **DoS** tab.
3. Toggle the status of **Enable Denial of Service prevention**, as needed.
4. Click **Save**.

5.6.4 Understanding Directory Harvest Attack Prevention

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

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

5.6.4.1 How MailMarshal Prevents Attacks

MailMarshal helps to prevent DHAs by the following means:

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

Copyright © 2026 Trustwave Holdings, Inc.

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

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

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



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

5.6.4.2 DHA Prevention Settings

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

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

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

5.6.5 Preventing Directory Harvest Attacks

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

To configure DHA prevention:

1. Create a list of all valid recipients by completing the following steps:

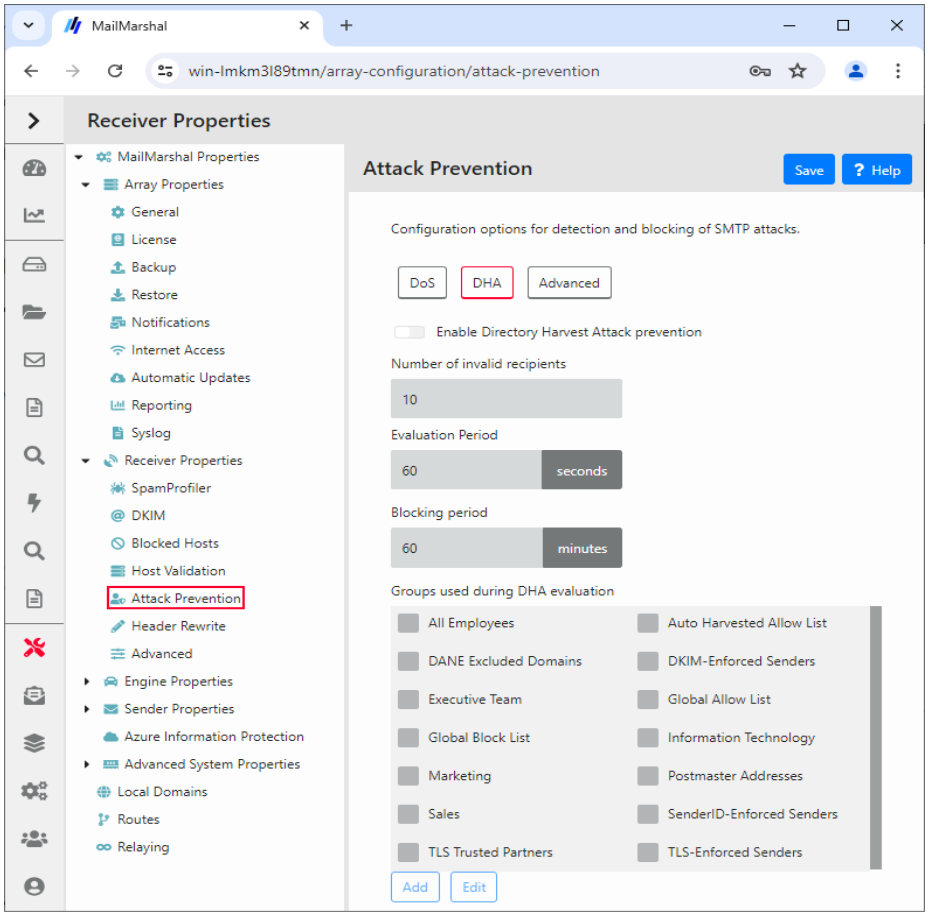
Copyright © 2026 Trustwave Holdings, Inc.

a. Create one or more Azure Entra, Active Directory or LDAP user groups that together contain all the user email addresses in your environment. For more information, see “Creating and Populating User Groups” on page 127.

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

b. Select these groups (or a group containing them) when configuring DHA prevention in the following steps.

2. In the Management Console, select **System Configuration** and then expand **Receiver Properties.**
3. Select **Attack Prevention** in the right pane menu, and select the **DHA** tab.
4. Select (toggle on) **Enable Directory Harvest Attack prevention**, and specify appropriate values. Specify the group(s) you created to be used during evaluation. For more information about the fields and settings, click **Help**.



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

Copyright © 2026 Trustwave Holdings, Inc.

5.6.6 Enabling and Disabling Directory Harvest Attack Prevention

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

To enable or disable DHA prevention:

1. In the Management Console, select **System Configuration** and then expand **Receiver Properties**
2. Select **Attack Prevention** in the right pane menu, and select the **DHA** tab.
3. Toggle the status of **Enable Directory Harvest Attack prevention**, as needed.
4. Click **Save**.

5.7 Filtering Messages and Attachments

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

A MailMarshal email policy is divided into Connection Policy, Content Analysis Policy, and Dead Letter Policy. Each of these sections contains one or more policy groups. Each policy group consists of one or more rules.

For more information about the options available when creating policy groups and rules, see “Understanding Policy Groups” on page 89 and “Understanding Rules” on page 90.

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

Connection Policies

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

Anti-Malware (Inbound)

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

Anti-Malware (Outbound)

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

Anti-Spam

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

Copyright © 2026 Trustwave Holdings, Inc.

Blended Threats

Contains rules that implement detection of suspect URLs in messages and attachments. Checking can be performed at the time of message processing. With the optional Blended Threat Service, checking can be performed at the time a link is clicked by the email recipient.

Attachment Management (Inbound)

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

Attachment Management (Outbound)

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

Policy Management (Inbound)

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

Policy Management (Outbound)

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

Automated Responses

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

Message Archiving

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

Copyright © 2026 Trustwave Holdings, Inc.

6 Understanding Email Policy, Policy Groups, and Rules

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

The Email Policy includes Connection Policy, Content Analysis Policy, and Dead Letter Policy. Each type of policy consists of one or more policy groups. Each policy group contains one or more rules. Each rule has three parts: User Matching, Conditions, and Actions.

MailMarshal applies Connection Policy while receiving a message. It applies Content Analysis Policy to each message after it is fully received. MailMarshal uses Dead Letter Policy to handle messages that cannot be unpacked or processed due to errors in formatting.

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

6.1 Understanding Policy Types

MailMarshal email policy is divided into Connection Policy, Content Analysis Policy, and Dead Letter Policy. Each Policy Group and Rule belongs to one of these types of policy.



Note: Connection Policy was previously known as Receiver Rules. Content Analysis Policy was previously known as Standard Rules.

6.1.1 Connection Policy

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

6.1.2 Content Analysis Policy

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

6.1.3 Dead Letter Policy

MailMarshal applies Dead Letter Policy when a message cannot be unpacked, or cannot be processed, due to errors in message formatting. By default these messages are quarantined in

Copyright © 2026 Trustwave Holdings, Inc.

special folders. You can specify a limited number of actions to deliver some of these messages to their original destination or an alternate address.

6.2 Understanding Policy Groups

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

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

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

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

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

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

To create a policy group:

1. In the left pane of the Management Console, select **Email Policy** and then select a type of policy.
2. Click **Add**.
3. On the General tab, enter a name and optional schedule information for this policy group.



Note: Scheduling is not available for Dead Letter Policy Groups.

4. On the Filtering tab, select the User Matching conditions for this policy group. If MailMarshal needs more information to define a condition, the description of the condition includes a hyperlink. Click the hyperlink to open a user matching condition panel that allows you to enter the required information.

Copyright © 2026 Trustwave Holdings, Inc.

6.3 Understanding Rules

MailMarshal Rules define filtering policy in detail. Rules include three basic sections: User Matching, Conditions, and Actions. User matching and scheduling also depend on the definition of the parent Policy Group.

6.3.1 Creating Rules

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

To create a rule:

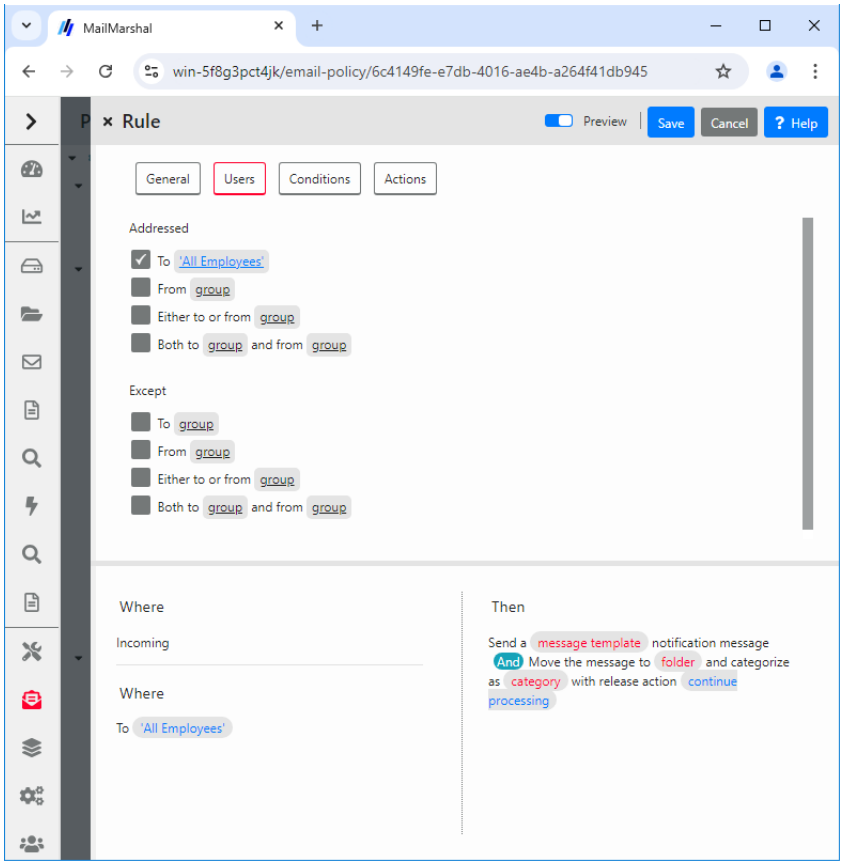
1. In the left pane of the Management Console, select **Email Policy**.
2. Expand Connection Policy, Content Analysis Policy, or Dead Letter Policy, and select a Policy Group.
3. Choose **Add** from the list menu to open rule properties. The properties panel includes four tabs that allow you to select conditions and actions. If MailMarshal needs more information to define a condition or action, the description of the item includes a hyperlink. Click the hyperlink to open a panel that allows you to enter the required information.



Tip: To see a list of all conditions and actions, enable **Preview** using the toggle at top right of the panel.

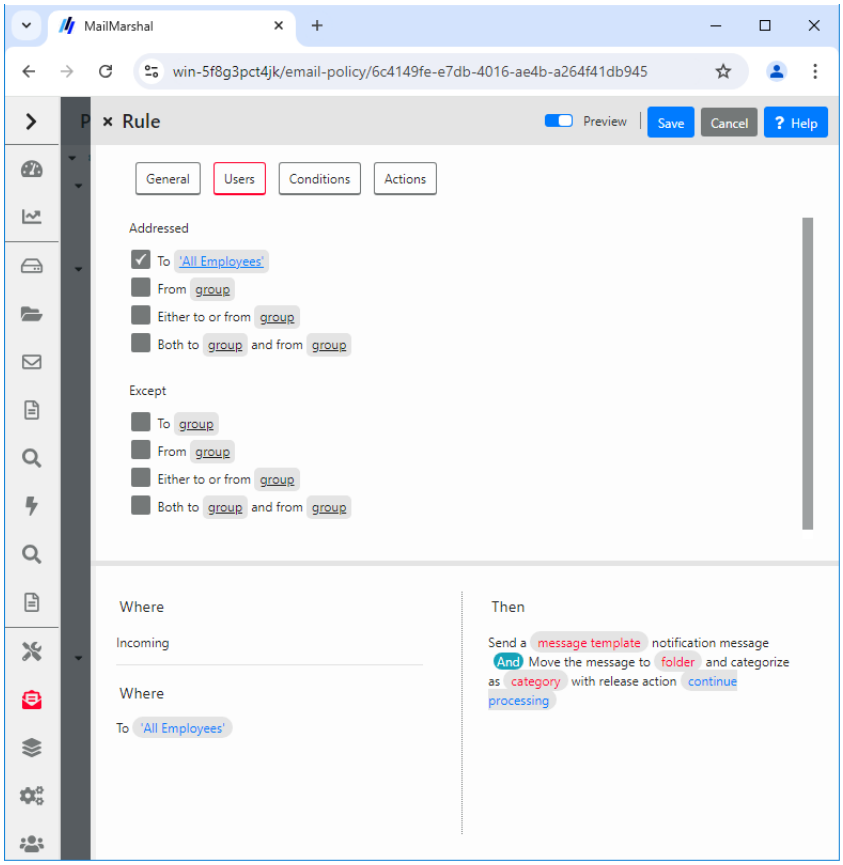
4. On the **General** tab, enter a name and optional description for this policy rule.
5. On the **Users** tab, select the User Matching conditions for this rule.

Copyright © 2026 Trustwave Holdings, Inc.



6. On the **Conditions** tab, select the conditions for this rule and specify any additional information required as for Step **4**.
7. On the **Actions** tab, select the actions for this rule and specify any additional information required as for Step **4**.
8. To create the rule, click **Save**.

Copyright © 2026 Trustwave Holdings, Inc.



6.4 Understanding User Matching

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

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 message is incoming

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

Where message is outgoing

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

Copyright © 2026 Trustwave Holdings, Inc.

Where addressed to group

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



Note: Whenever a condition requires a “group,” the list can contain individual email addresses, wildcard patterns to match sets of addresses such as domains, and MailMarshal user groups. Certain “From” conditions can also contain MailMarshal IP Groups. Conditions that use the same group list to match both “To” and “From” do not allow IP Group matching.

For more information about wildcard characters, see “Wildcard Characters” on page 220.

For more information about which email addresses in a message MailMarshal checks, see Knowledgebase article Q12238.

Where addressed from group

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

Where addressed either to or from group

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

Where addressed both to group and from group

Requires two lists of groups. Allows IP groups in the “From” clause. Matches if the recipient of the message is found in the first list of groups specified, and the sender of the message is found in the second list of groups specified.

Except where addressed to group

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

Except where addressed from group

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

Except where addressed either to or from group

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

Except where addressed both to group and from group

Requires two lists of groups. Allows IP groups in the “From” clause. Matches if the recipient of the message is **not** found in the first list of groups specified, and the sender of the message is **not** found in the second list 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 incoming except where addressed to Managers`.

Copyright © 2026 Trustwave Holdings, Inc.

6.5 Understanding Rule Conditions

MailMarshal evaluates rule conditions within each rule. 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 in the Management Console. If the condition includes options, arguments, or variables, you can click a hyperlink in the rule edit panel to open a panel that allows you to specify values.



Note: Many conditions allow you to choose a positive or negative match (trigger the condition if the selected criteria are matched, or not matched). This option may be available as a separate link or within the main condition. Rule negation ("does not match") can be useful to control the flow of rule evaluation. However negation of a complex condition should be carefully considered and tested to avoid unwanted results.

6.5.1 Rule Conditions for Content Analysis Policy Rules

The following conditions are available for use in Content Analysis Policy rules. They are further explained in the sections following.

- **Security**
  - Where message is/is not detected as spam by SpamEngine
  - Where the result of a virus scan is/is not
  - Where message is/is not identified as containing malware by Yara Analysis Engine script
  - Where message does/does not contain suspect URLs
  - Where message does/does not appear to be spoofed based on criteria
  - Where message does/does not trigger TextCensor script(s)
- **Message Attachments**
  - Where message attachment is/is not of type
  - Where attachment fingerprint is/is not known
  - Where message does/does not contain attachment(s) named (file names)
  - Where attachment parent is of type
  - Where the attached image does/does not/may match image category
- **Size**
  - Where message size is
  - Where the estimated bandwidth required to deliver this message is
  - Where message attachment size is
  - Where number of recipients is count
  - Where number of attachments is count
- **Sender**

Copyright © 2026 Trustwave Holdings, Inc.

  - Where the sender is/is not in the recipient's safe senders list
  - Where the sender is/is not in the recipient's blocked senders list
  - Where sender's IP address does/does not match address
  - Where sender did/did not authenticate successfully
- **TLS**
  - Where message was/was not received via TLS
  - Where message was/was not received via TLS versions
  - Where the TLS client certificate was/was not presented with criteria
- **Other**
  - Where the external command is/is not triggered
  - Where message does/does not contain one or more headers (header match)
  - Where message does/does not trigger category script(s)
  - Where the DKIM verification result is
  - Where message was checked with DMARC and a result applied



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

6.5.1.1 Where message is/is not detected as spam by SpamEngine

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

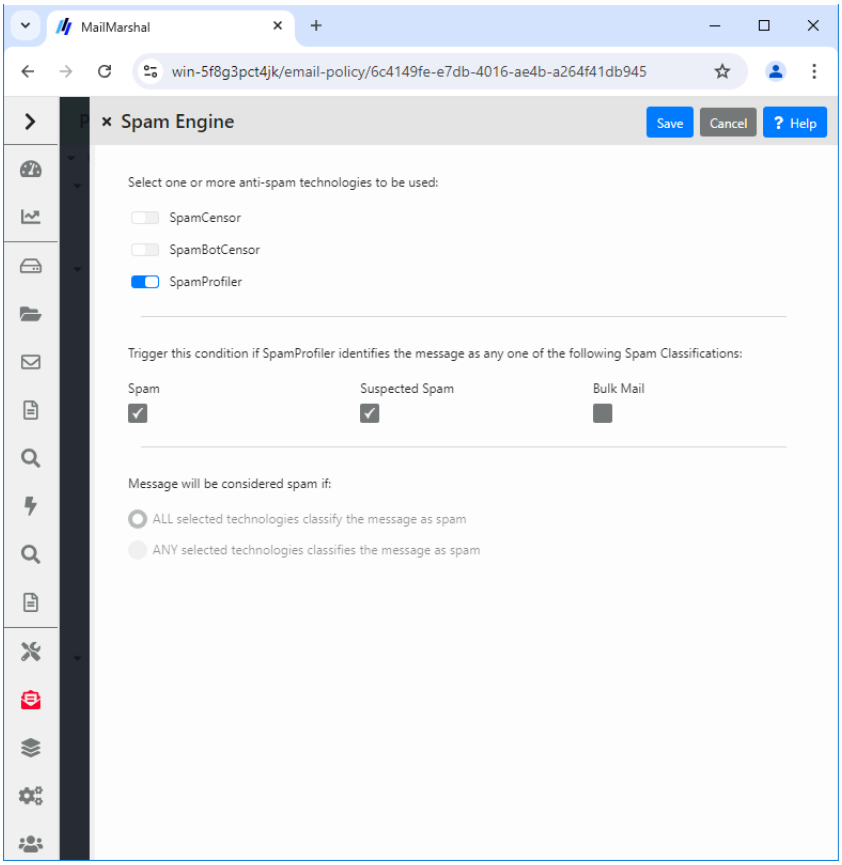


Note: You can also choose to reject messages at the Receiver based on SpamProfiler evaluation. For more information, see "Configuring SpamProfiler" on page 72.

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

Copyright © 2026 Trustwave Holdings, Inc.

On the rule condition panel, select the anti-spam technologies you want to use.



- If you select SpamProfiler, you can select one or more sub-classifications to check. The Spam-Profiler evaluation triggers if any of the sub-classifications triggers.
- You can choose to trigger the condition if all or any of the technologies classifies the message as spam.

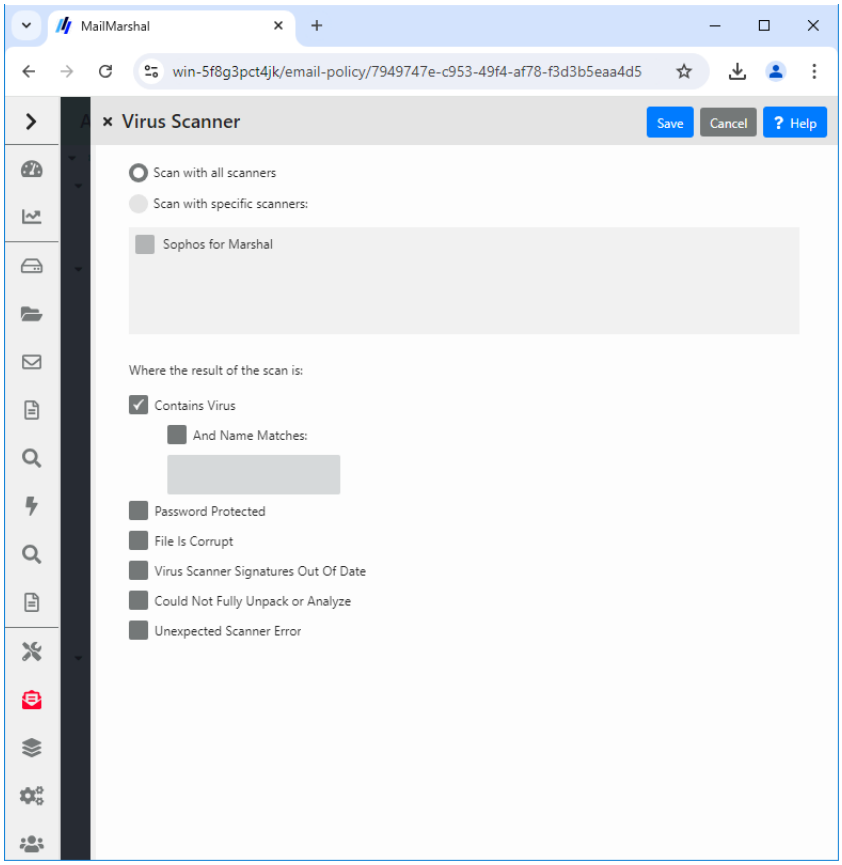
For more information, see Help.

6.5.1.2 Where the result of a virus scan is/is not

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

Copyright © 2026 Trustwave Holdings, Inc.

Figure 11: Virus scanning rule condition



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

- **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.

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 panel.

- **Contains Virus:** The condition will trigger if any part of the message contains a virus. This is the basic condition.
- **...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 220 and “Regular Expressions” on page 221.
- **Password Protected:** When you select this item, the condition will trigger if the scanner reports the file as password protected.

Copyright © 2026 Trustwave Holdings, Inc.

- **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 panel 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. For command line scanners, configure the list of return codes in the virus scanner properties. For more information about virus scanner properties, see “Using Virus Scanning” on page 154.

6.5.1.3 Where message is/is not identified as containing malware by Yara Analysis Engine

This condition allows you to take action on a message based on the result of evaluation by the proprietary Yara Analysis Engine (YAE). This technology provides an additional layer of protection against malware and other spam messages.

You can use this condition in combination with other conditions to fine-tune recognition of malware. The rule condition panel allows you to select a specific Yara Analysis Engine script for use in this condition.



Note: MailMarshal includes a default rule to check messages and attachments using a YAE script that is provided by the LevelBlue SpiderLabs Email Security team and automatically updated (`AMAX.yae`). Advanced administrators can create custom YAE scripts. For more information, see the document “Using Yara Analysis Engine Scripts”, available from the MailMarshal support page on the LevelBlue website.

6.5.1.4 Where message does/does not contain suspect URLs

This condition extracts URLs from the message and checks them against a list of suspect URLs maintained by LevelBlue and constantly updated from a variety of trusted sources.



Note: To improve overall performance, place rules that use this criterion after spam blocking rules, and before rules that rewrite URLs for Blended Threat analysis.

6.5.1.5 Where message does/does not appear to be spoofed based on criteria

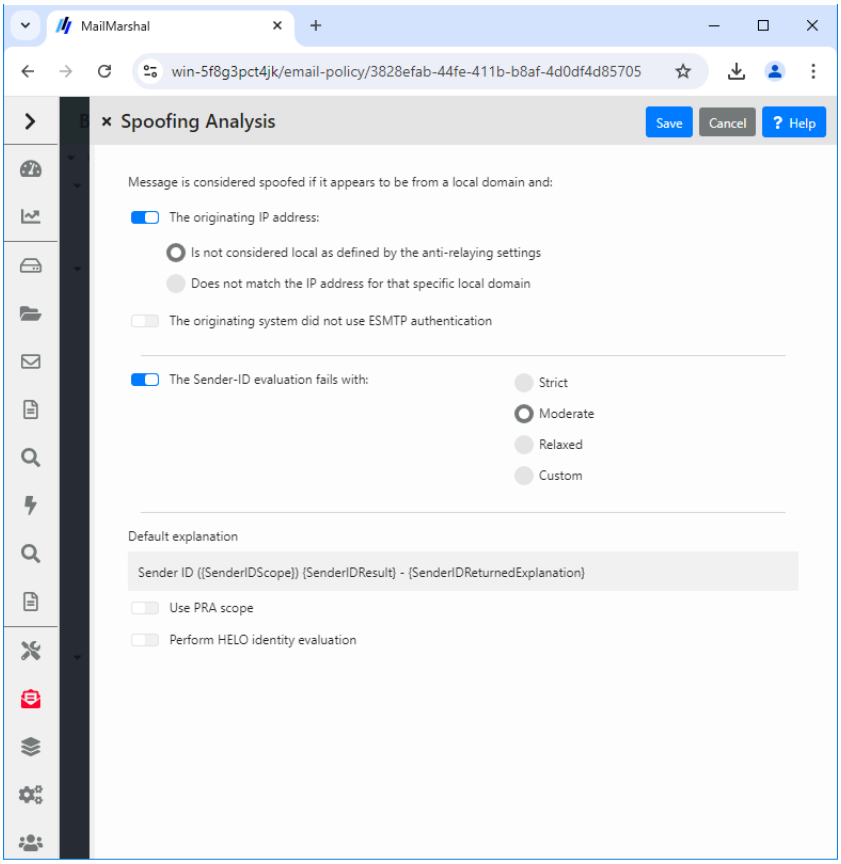
This condition allows you to define when MailMarshal should consider a message to be spoofed. A **spoofed** message did not originate within the domain of the claimed sender email address.

Copyright © 2026 Trustwave Holdings, Inc.

MailMarshal can check spoofing based on local domain servers, authenticated connections, and/or Sender ID.

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

Figure 12: Message spoofing analysis rule condition



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 in the **System Configuration > Local Domains** item in the Management Console. 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 in the MailMarshal Relaying Table that is effective from this server. This option is useful if you allow multiple servers and workstations in the local network to route email directly through MailMarshal.

Copyright © 2026 Trustwave Holdings, Inc.

- 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 computer 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 the 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 local users from "spoofing" addresses within the local domains.

The originating system did not use ESMTP authentication:

Select this option to check for spoofing based on the login given by the system that delivered the message to MailMarshal. Use this condition (and not an IP address based condition) if you allow roving users to send email through MailMarshal using the Authentication feature. For more information about this feature see "Authentication by Account" on page 81.

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

The Sender-ID evaluation fails:

Select this option to evaluate the message using the Sender ID Framework. Click **Change Settings** to see additional settings that allows you to configure detailed Sender ID criteria.



Note: For more information about Sender ID, see Knowledgebase article Q11559.

6.5.1.6 Where message did/did not trigger TextCensor 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 scripts.

In the rule condition panel, you can select one or more TextCensor scripts to be used in evaluating the message. You can add a script or edit an existing script. For detailed information about Scripts, see "Identifying Email Text Content Using TextCensor Scripts" on page 130.



Note: You can include more than one TextCensor script in this condition by selecting multiple boxes in the rule condition panel. By default if you select more than one script, all the scripts you select must trigger for the condition to be true (logical AND). You can choose to make the condition true if ANY script triggers (logical OR).

6.5.1.7 Where message attachment is/is not of type

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

Copyright © 2026 Trustwave Holdings, Inc.

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

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

6.5.1.8 Where attachment fingerprint is/is not known

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

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

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

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

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

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

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

Files can also be “made known” by placing them in the ValidFingerprints sub-folder of the Quarantine folder on any email processing server. MailMarshal loads these fingerprints every 5 minutes, and when configuration is committed. For further information about this process, see Knowledgebase article Q10543.

6.5.1.9 Where message does/does not contain 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 panel. 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.

Copyright © 2026 Trustwave Holdings, Inc.

6.5.1.10 Where attachment parent is of type

This condition is intended to be used with the condition "Where message did/did not trigger TextCensor script(s)." 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 MS Word document.

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

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

6.5.1.11 Where the attached image does/does not/may match image category

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).

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

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

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

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

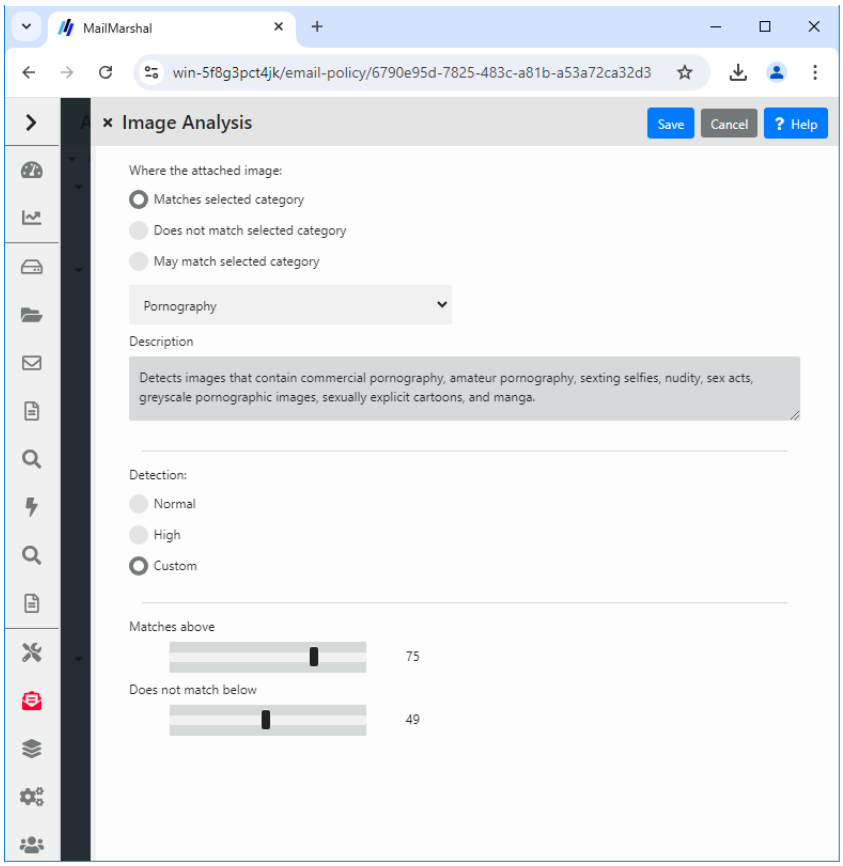
Image Analyzer actually scans files of the following types: BMP, DIB, JPEG, JPG, JPE, J2K, JBG, JPC, PNG, PBM, PGM, PPM, SR, RAS, TIFF, TIF, GIF, TGA, WMF, PGX, PNM, RAS. For more information see Knowledgebase article Q11622.

MailMarshal does not request image analysis for very small images (by default, images smaller than 75x75 pixels). You can adjust this setting. See Knowledgebase article Q14960.

Copyright © 2026 Trustwave Holdings, Inc.

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

Figure 13: Image analysis rule condition



The attached image matches selected category:

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

The attached image does not match selected category:

Specifies that the condition will trigger if Image Analyzer returned a score below the “does not match below” value.

The attached image may match selected category

Specifies that the condition will trigger if Image Analyzer returned a score between the “matches above” and the “does not match below” values.

Category selection

Specifies a single Image Analyzer category to be checked in this rule condition. The **Description** field shows the intended purpose of the selected category. To check for additional categories, use one rule per category.

Copyright © 2026 Trustwave Holdings, Inc.

In the **Detection** section you can configure advanced settings for Image Analyzer.

You can choose from the following basic detection settings:

Normal:

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

High:

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

Custom:

Allows you to set the Image Analyzer triggering levels using the slider controls.

- Matches above: Specifies the minimum Image Analyzer return value that causes an image to be classified as matching the selected category, for example, likely to be pornographic. Default value: 75 for “normal” setting; 60 for “high” setting.
- Does not match below: Specifies the maximum Image Analyzer return value that causes an image to be classified as not matching the selected category. Default value: 49.



Notes:

- MailMarshal versions prior to 10.1 used only the “Pornography” category. Any rules upgraded from those earlier versions use this category.
- Some earlier product versions included additional sensitivity settings. These settings are no longer required.

6.5.1.12 Where message size is

MailMarshal uses the size of the entire message, before unpacking, in this condition. The rule condition panel 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.

6.5.1.13 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 panel 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.

Copyright © 2026 Trustwave Holdings, Inc.

6.5.1.14 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 panel 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.

6.5.1.15 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 panel 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.



Tip: This condition is evaluated based on the RCPT TO list specified when the message was received. It does not check the content of email headers such as To:, CC:, or BCC:.

6.5.1.16 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 panel 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.

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

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

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

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



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

Copyright © 2026 Trustwave Holdings, Inc.

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

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

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

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



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

6.5.1.19 Where sender's IP address does/does not match 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 Connection Policy rules. To save resources and improve security, you should use this condition in a Connection Policy rule where possible.

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

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

- **An IP Address:** Enter a single IPv4 or IPv6 address. For instance, enter "10.2.0.4" or "::1".
- **A range of IP addresses:** Enter the starting and ending IP addresses for an inclusive range. For instance, enter "10.2.1.4" and "10.2.1.37"
- **An entire network range:** Enter an IP address and a network mask in CIDR notation. For instance, enter "10.2.1.4" and "24" to match the entire 10.2.1.0 subnet. Enter "fe80::" and "10" to match IPv6 link-local addresses.

The check box at the bottom of the panel 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.

Copyright © 2026 Trustwave Holdings, Inc.

6.5.1.20 Where sender did/did not authenticate successfully

This condition can be used to check whether MailMarshal authenticated the remote system using an account and password. For more information about setting up accounts for authentication see “Setting Up Accounts” on page 191.



Note: You can also check for authentication using the Connection Policy rule condition “Where sender has authenticated.” To save resources and improve security, you should use the Connection Policy condition where possible. Using a Content Analysis policy rule allows more actions and combinations of conditions.

6.5.1.21 Where message was/was not received via TLS

This condition allows you to take action on messages depending on whether they were received with TLS (Transport Layer Security). For more information about setting up TLS in MailMarshal, see “Securing Email Communications” on page 198.

6.5.1.22 Where message was/was not received via TLS versions

This condition allows you to take action on messages depending on the version of TLS used to secure the connection. For more information about setting up TLS in MailMarshal, see “Securing Email Communications” on page 198.

6.5.1.23 Where the TLS client certificate was/was not presented with criteria

This condition allows you to take action on messages depending on the specific features of the SSL certificate that was used to secure the connection. You can check the date, trust, revocation status, and other features. For full details of the available options, see Help. For more information about setting up TLS in MailMarshal, see “Securing Email Communications” on page 198.

6.5.1.24 Where the external command is/is not 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 panel, specify the commands. If more than one command is specified, all commands must be triggered for this condition to be triggered. For more information about external commands see “Extending Functionality Using External Commands” on page 163.

6.5.1.25 Where message does/does not contain 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 panel, click **Add** to create a new header match rule. For more information about creating header match rules, see “Using Rules to Find Headers” on page 159.

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.

Copyright © 2026 Trustwave Holdings, Inc.

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

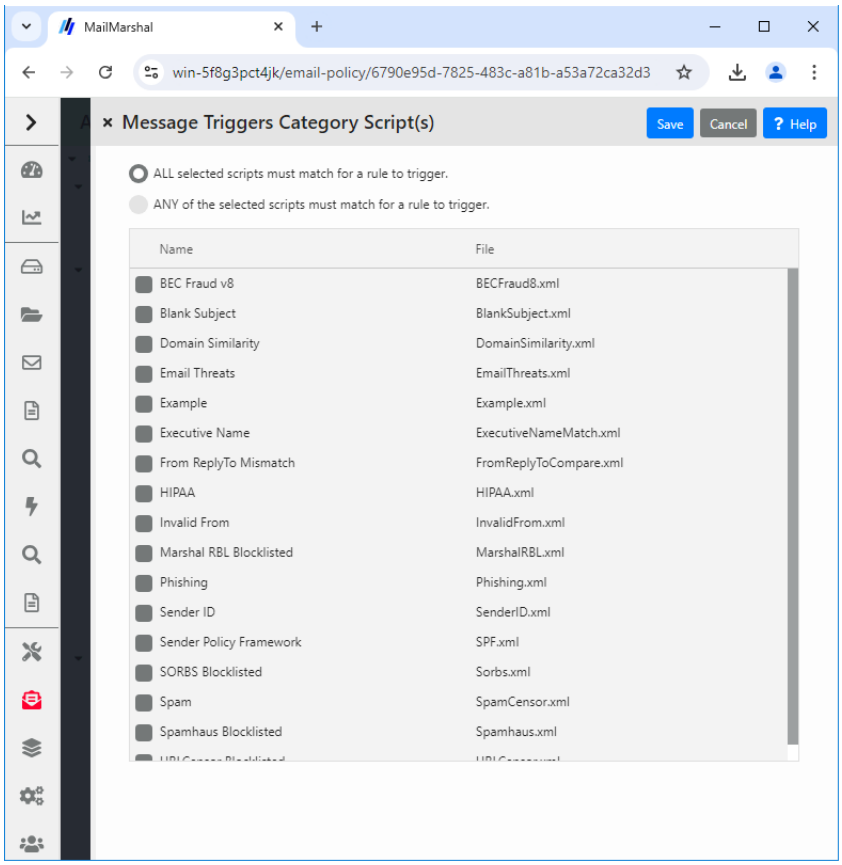
Note: You can only use Header Match conditions within the rule where you create them. To use the same condition in more than one rule, create it in each rule.

6.5.1.26 Where message does/does not trigger category script(s)

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

If you select more than one script, you can choose to take action if all scripts trigger, or if any of the scripts trigger.

Figure 14: Category script rule condition



MailMarshal can automatically download updates to category scripts.

You can create and customize your own category scripts. Some example category scripts are provided with MailMarshal. For more information, see the technical reference “MailMarshal Anti-Spam Configuration,” available from the MailMarshal support page on the LevelBlue website.

Copyright © 2026 Trustwave Holdings, Inc.

6.5.1.27 Where the DKIM verification result is

This condition allows you to take action on messages depending on the results of DKIM (DomainKeys Identified Mail) validation. You can choose to take action on messages that pass or fail validation, on messages where the required information could not be retrieved, or on messages where the DKIM header was not present.



Note: DKIM validation of the message is performed when the message is received. To use this condition, you must enable DKIM validation (in System Configuration, see **MailMarshal Properties > Array Properties > Receiver Properties > DKIM**).

6.5.1.28 Where message was checked with DMARC and a result applied

This condition allows you to take action on messages depending on the results of DMARC (Domain-based Message Authentication, Reporting & Conformance) validation. You can choose to take action on messages that pass validation, messages that could not be evaluated, and messages that fail validation. For messages that fail DMARC validation, you can base the action on the DMARC policy of the sending domain. For full details of the available options, see Help.

6.5.2 Rule Conditions for Connection Policy Rules

The following conditions are available for use in Connection Policy rules.

- **General**
  - Where message is of a particular size
  - Where SPF evaluation is
- **Sender**
  - Where sender’s HELO name is/is not criteria
  - Where sender's IP address does/does not match address
  - Where sender did/did not authenticate successfully
  - Where sender's IP address is/is not listed by Reputation Service
- **TLS**
  - Where message was/was not received via TLS
  - Where message was/was not received via TLS versions
  - Where the TLS client certificate was/was not presented with criteria

6.5.2.1 Where message is of a particular size

This condition is normally used with a “refuse message” action to refuse large messages. The rule condition panel allows you to choose a size and matching method (greater than a given size, less

Copyright © 2026 Trustwave Holdings, Inc.

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 Content Analysis Policy rule to include messages received from sources that do not support ESMTP. See also Knowledgebase article Q10602.

6.5.2.2 Where 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.

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

See Help for definitions of the options.



Note: For more information about SPF, see Knowledgebase article Q11560.

6.5.2.3 Where sender's HELO name is/is not criteria

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

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



Note: You can check one or more of the boxes.

Matching of a specific string supports wildcards. For more information, see “Wildcard Characters” on page 220.

6.5.2.4 Where sender's IP address does/does not match 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 panel. To add a range to the list, click **New** to open the Match IP Address panel. To modify an existing address, highlight it, and then click **Edit.** To delete an existing address from the list, highlight it, and then click **Delete**.

Copyright © 2026 Trustwave Holdings, Inc.

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

- **An IP Address:** Enter a single IPv4 or IPv6 address. For instance, enter “10.2.0.4” or “::1”.
- **A range of IP addresses:** Enter the starting and ending IP addresses for an inclusive range. For instance, enter “10.2.1.4” and “10.2.1.37”
- **An entire network range:** Enter an IP address and a network mask in CIDR notation. For instance, enter “10.2.1.4” and “24” to match the entire 10.2.1.0 subnet. Enter “fe80::” and “10” to match IPv6 link-local addresses.

The check box at the bottom of the panel 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.

6.5.2.5 Where sender did/did not authenticate successfully

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 “Setting Up Accounts” on page 191.



Note: You can also check for authentication using the Connection Policy rule condition “Where sender did/did not authenticate successfully.” To save resources and improve security, you should use the Connection Policy condition where possible. Using a Content Analysis policy rule allows more actions and combinations of conditions.

6.5.2.6 Where sender's IP address is/is not listed by Reputation Service

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

The panel shows a list of all configured services. Select the check box for each service you want to use. Clear the check box for any service you do not want to use in this Condition. For information about how to configure reputation services, see “Reputation Services and DNS Blocklists” on page 78.



Note: Reputation Services results are based on the IP address of a server, and currently provide information about IPv4 addresses only.

6.5.2.7 Where message was/was not received via TLS

This condition allows you to take action on messages depending on whether they were received with TLS (Transport Layer Security). For more information about setting up TLS in MailMarshal, see “Securing Email Communications” on page 198.

Copyright © 2026 Trustwave Holdings, Inc.

6.5.2.8 Where message was/was not received via TLS versions

This condition allows you to take action on messages depending on the version of TLS used to secure the connection. For more information about setting up TLS in MailMarshal, see “Securing Email Communications” on page 198.

6.5.2.9 Where the TLS client certificate was/was not presented with criteria

This condition allows you to take action on messages depending on the specific features of the SSL certificate that was used to secure the connection. You can check the date, trust, revocation status, and other features. For full details of the available options, see Help. For more information about setting up TLS in MailMarshal, see “Securing Email Communications” on page 198.

6.5.3 Rule Conditions for Dead Letter Policy Rules

The following conditions are available for use in Dead Letter Policy rules:

- Where the dead letter reason contains
- Where message is detected as spam by SpamProfiler

6.5.3.1 Where the Dead Letter reason contains

This condition allows you to enter text that MailMarshal will match in the Dead Letter Reason field of a deadlettered message. You can choose to allow a deadlettered message to be passed through to recipients. For a list of the reason codes, see Knowledgebase article Q14226.

6.5.3.2 Where message is detected as spam by SpamProfiler

This condition allows you to take action on a deadlettered message based on the result of evaluation by SpamProfiler. You can use this condition to classify deadlettered messages as spam, or move them to the deadletter spam folder.



Note: The SpamCensor and SpamBotCensor engines cannot be used to evaluate deadlettered items because they can only evaluate a fully unpacked message.

6.6 Understanding Rule Actions

MailMarshal rule actions are performed by each rule. 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.

6.6.1 Rule Actions for Content Analysis Policy Rules

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

- **Logging and Notification**

Copyright © 2026 Trustwave Holdings, Inc.

- Send a notification message
- Log message with classifications
- Report the DMARC policy disposition
- Copy the message to folder with release action
- Do not generate an NDR if the remote host refuses the message
- Run the external command

- **Data Harvesting**
  - Add message users into group
  - Add attachments to valid fingerprints list
- **Message Modification**
  - Stamp message with message stamp
  - Strip attachment
  - Rewrite message headers
  - Prepend text to message subject
  - Rewrite URLs in the message for Blended Threat Scanning
- **Routing and Delivery**
  - Send a copy of the message to host
  - BCC a copy of the message
  - Deliver the mail via TLS only
  - Set message routing to host
  - Ignore DANE validation
  - Apply DKIM signature
- **Terminal Actions**



Tip: You must select exactly one Terminal Action for each rule.
To apply additional rules to a message, select **Pass the Message to Rule** or **Continue Processing**.

  - Move the message to folder and categorize, with release action
  - Park the message
  - Hold the message
  - Delete the message and categorize
  - Pass the message to rule
  - Continue Processing

Copyright © 2026 Trustwave Holdings, Inc.

6.6.1.1 Send a notification message

This action sends one or more email messages based on the templates selected in the rule action panel. To view or edit the details of a particular template, select it, and then click **Edit Template**. To create a new template, click **New Template.** The new template will automatically be selected for use when you return to the template selection panel. For further information about templates, see “Notifying Users with Message Templates and Message Stamps” on page 142.

6.6.1.2 Log message with classifications

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

Select one or more logging classifications from the list in the rule action panel. Select the check box to write a logging classification for every component of the message (for example a separate record for each image file in a message). To view or edit the detailed information in the classification, click **Edit** in the selection panel. To create a new classification, click **New** in the selection panel. For details on classifications, see “Using Folders and Message Classifications” on page 154



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

6.6.1.3 Copy the message

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

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

When you select this action you can create a new folder. To create a folder, click **New Folder**. For more information see “Using Folders and Message Classifications” on page 154.

6.6.1.4 Report the DMARC Policy Disposition

This action allows you to specify the DMARC disposition that MailMarshal will report to the Domain Owner in DMARC aggregate reports. Select the appropriate disposition (None, Quarantine, or Reject).

6.6.1.5 Do not generate an NDR if the remote host refuses the message

This action allows you to avoid sending NDR messages. This action could be used for inbound messages where MailMarshal has a valid list of accepted recipients and is responsible for sending NDRs. In this situation any refusal from the internal mail server is taken as an error or unexpected blockage that should not be reported to the sender.



Note: This action should not be applied to outgoing messages.

Copyright © 2026 Trustwave Holdings, Inc.

6.6.1.6 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.

Choose one or more commands to be run from the list of pre-defined external commands. For information about defining external commands, see “Extending Functionality Using External Commands” on page 163. To run the same application with different parameters under different conditions, use more than one external command definition.

You can also choose to repack the message when a command action succeeds. Use this setting if you have created a custom external command that could make changes to the message content.



Tip: To minimize processing overhead, only repack when required. For more details see Help.

6.6.1.7 Add attachments to valid fingerprints list

This action adds the attachments to the MailMarshal list of “valid fingerprints” (normally used for images or other files which require special treatment, such as company logos). In the rule action panel, choose whether to add all attachments, or only images, to the list. For more information, see the rule condition “Where attachment fingerprint is/is not known.”

6.6.1.8 Add message users into group

This action allows you to add members to a MailMarshal user group based on any rule criteria, such as the sender or recipients of a message. You can use this action to automate the generation of lists of safe senders or blocked senders, based on other features of messages.



Note: When you use this action to add members to a group, you should consider enabling automatic pruning to limit the size of the group. See “Pruning a MailMarshal Group” on page 128.

In the rule action panel, select one or more groups MailMarshal should add users to. Choose whether to add the sender or recipients.

You can create a new group by clicking **New Group.**

6.6.1.9 Stamp message with text

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

In the rule action panel, choose one or more message stamps to be used. A stamp will add text at the top or bottom of the message as selected when it is created. To view or edit the details of a particular message stamp, select it, and then click **Edit Stamp**. To create a new stamp, click **New Stamp**; the new message stamp will automatically be selected when you return to the stamp selection panel. For details on message stamps, see “Notifying Users with Message Templates and Message Stamps” on page 142.

Copyright © 2026 Trustwave Holdings, Inc.

6.6.1.10 Strip attachment

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



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.

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

6.6.1.11 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 panel, click **Add** to create a new header rewrite rule. For more information about this adding and editing header rewrite rules, see “Using Rules to Change Headers” on page 160.

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 panel will be evaluated first. Adjust the order of evaluation by selecting a rule and using the up and down arrows on the panel.



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 Receiver), create a Header Rewrite rule in each place.

6.6.1.12 Prepend text to message subject

Use this action to add text at the beginning of the message subject. You can use this action to provide results of message scanning (such as “external sender” or “suspect spam”) in a way that the recipient will easily see.

6.6.1.13 Rewrite URLs in the message for Blended Threat Scanning

This action can be used to protect users against malicious websites listed in the LevelBlue Blended Threats URL database. The action modifies web links (URLs) in the subject and body of email messages, so that when a user clicks the link, the URL is tested by the LevelBlue Blended Threat service.

Copyright © 2026 Trustwave Holdings, Inc.

This action can only be used in rules that affect inbound messages (messages addressed to your local domains).



Note: If the Blended Threats service is not licensed, you cannot save a rule that uses this condition.

You can exclude trusted URL domains from rewriting and scanning. For more information, see “MailMarshal Properties – Advanced” on page 200.

For information about what is rewritten and what is excluded from rewriting by default, see Knowledgebase article Q14548.

For more information about Blended Threats Scanning, see Knowledgebase article Q12876.

6.6.1.14 Send a copy of the message to host

This action sends a copy of the message to a specific server. Unlike the BCC action, this action does not modify the recipient fields.

In the rule action panel, enter a host name or IP address, and a port number, to which MailMarshal should send the message. If you entered a host name, select a protocol to use for delivery (IPv4, IPv6, or either).



Tip: You can use this action to provide a true copy to an external service.

6.6.1.15 BCC a copy of the message

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



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

6.6.1.16 Deliver the mail via TLS only

This action allows a message to be marked for sending using TLS. If the message cannot be delivered using TLS for any recipient, it will not be sent to that recipient. You can use this action to implement specific TLS requirements based on any rule condition such as the sender, recipient, or message content.

You can also require TLS for messages sent to all users in specific domains. See **MailMarshal Properties > Array Properties > Sender Properties > Outbound Security (TLS)**.



Note: This action is not a terminal action. It sets the requirement of TLS delivery for the message, but it does not send the message immediately or stop rule evaluation. MailMarshal continues to evaluate remaining applicable rules.

Copyright © 2026 Trustwave Holdings, Inc.

6.6.1.17 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 panel, enter a host name or IP address, and a port number, to which MailMarshal should send the message. If you entered a host name, select a protocol to use for delivery (IPv4, IPv6, or either). MailMarshal uses this address when it attempts delivery, even if the message is "parked" first, or quarantined and later released. If several rules invoke this action, MailMarshal 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.

If you are integrating MailMarshal and MailMarshal Secure Email Server (for encryption and decryption processing), check the box *This is a MailMarshal Secure Email Server.*



Note: If you are not directing mail to a MailMarshal Secure Email Server, ensure this box is **not** checked. For more information about this feature, see the MailMarshal Secure Email Server User Guide.

6.6.1.18 Ignore DANE validation

This action allows you to skip DANE validation (when DANE is enabled). You can use this action in a rule with User Matching. The group used for matching should contain domain wildcard entries. For more information about using DANE with MailMarshal, see Knowledgebase article Q21213.

6.6.1.19 Apply DKIM signature

This action signs the message according to the DKIM standard. Signing of the message takes place after all rules are processed.



Note: Before using this action, you must import a private key for the local domain from which the message was sent. You must also publish public key information in a DNS TXT record so that signed messages can be validated. See "Configuring DKIM" on page 193.

You can set the action to take if signing does not succeed (continue processing, or move the message to a folder, and optionally send an email notification). For details of the settings, see Help.

6.6.1.20 Move the message and categorize

This action moves the email message file to the specified quarantine folder. To make the message processing log available in the same folder, select the check box at the bottom of the rule action panel. The message log explaining how the message was processed will then be available in the Console. If a new folder is required, click **Add** to open a panel that allows you to create a folder.

You can select a "category" that will be used to generate Dashboard graphs and other message statistics.

You can specify how MailMarshal will process the message by default if it is released from this folder. Click the **Release action** link to specify the action. By default when a message is released,

Copyright © 2026 Trustwave Holdings, Inc.

MailMarshal continues processing with the rule immediately after the rule that moved the message. For more information, see Help for the Release action panel.

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).

6.6.1.21 Park the message

This action moves the email message file to the specified parking folder for release according to the schedule associated with that folder. To create a new folder with a different schedule, click **Add** to open a panel that allows you to create a 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. When a message is released from a parking folder, MailMarshal continues processing with the rule after the rule that parked the message.

6.6.1.22 Hold the message

This action moves the email message file to a special "hold queue" for the specific rule. You can configure a hold period after which the message will be re-submitted to the rule that caused the hold.

You can configure the number of times MailMarshal should retry the rule before continuing to the next rule. For details of the settings, see Help.



Caution: Use this action only with a rule condition that can change when re-evaluated (such as scanner signature out of date conditions). If you use this action with a condition that never changes, affected messages will be delayed for no benefit.

This is a terminal action. If this action is performed, MailMarshal does not process any further rules for a message until the hold time expires. When a message is released from the hold queue, MailMarshal continues processing with the rule that caused the hold. If the number of retries is exceeded, MailMarshal continues processing with the rule after the hold rule.

You can force an immediate retry of held messages using the Hold Queues listing in the Console.

6.6.1.23 Delete the message

This action deletes the email message file. The message will not be sent to its original destination.

You can select a "category" that will be used to generate Dashboard graphs and other message statistics.

This is a terminal action. MailMarshal does not process any further rules for a message if this action is performed.

6.6.1.24 Pass the message to rule

This action allows a choice of which further rules to apply. Several choices are available in the rule action panel:

- Skip the next rule (do not apply it).
- Skip to the next policy group (do not apply further rules in this policy group).

Copyright © 2026 Trustwave Holdings, Inc.

- Skip all remaining rules (pass the message through to the intended recipients).
- Skip to a specific policy group or rule.



Note: It is only possible to skip to a rule which is evaluated after the current rule. The order of evaluation can be changed. See “Understanding the Order of Evaluation” on page 123.

When skipping to a rule in a different policy group, remember that the parent policy group conditions can prevent its having any effect. For instance, skipping from the MailMarshal default Policy Management (Inbound) policy group to the Policy Management (Outbound) policy group is allowed, but rules in the Outbound policy group will have no effect on inbound messages.

6.6.1.25 Continue processing

This action continues rule processing with the next listed rule.

6.6.2 Rule Actions for Connection Policy Rules

The following actions are available for use in Connection Policy rules.

- Accept message
- Refuse message and reply with message.



Note: These actions take effect immediately. If you use both types of actions in Connection Policy rules, check the order of evaluation carefully to ensure that MailMarshal checks for any exceptions first.

- Continue Processing Rules

6.6.2.1 Accept message

This action directs MailMarshal to accept the message for delivery subject to Content Analysis Policy rules. The message could be relayed to an address outside the MailMarshal 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.

6.6.2.2 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 Reputation Service conditions.

On the rule action panel, 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.

Copyright © 2026 Trustwave Holdings, Inc.

- **Message Description:** Enter a short message giving details of the reason for refusal. Within this message, the following variables are available:

Table 13: Variables for message description

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.

6.6.2.3 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.”

6.6.3 Rule Actions for Dead Letter Policy Rules

The following actions are available for use in Dead Letter Policy rules. Note that in some cases Dead Letter actions allow fewer options than the corresponding Content Analysis actions.



Caution: Messages that are dead lettered are **not scanned for viruses**, or checked by any other content rules (in most cases), because MailMarshal could not process them. If you choose to release or re-route these messages, ensure that the recipients are aware of the risks.

- **Logging and Notification**
  - Send a notification message
  - Write log message(s) with classifications
- **Routing and Delivery**
  - BCC a copy of the message
  - Set message routing to host
- **Terminal Actions**



Tip: You must select exactly one Terminal Action for each rule.

To apply additional rules to a message, select **Pass the Message to Rule** or **Continue Processing**.

  - Move the message to folder
  - Delete the message
  - Pass message through to recipients

6.6.3.1 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

Copyright © 2026 Trustwave Holdings, Inc.

semi-colons. You can also use variables in this field. The original message will not be modified in any way by this action, so the original recipient would not know a copy had been taken.



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

6.6.3.2 Send a notification message

This action sends one or more email messages based on the templates selected in the rule action panel. For further information about templates, see “Notifying Users with Message Templates and Message Stamps” on page 142.

6.6.3.3 Write log message(s) with classifications

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

Select one or more logging classifications from the list in the rule action panel. For details on classifications, see “Using Folders and Message Classifications” on page 154.



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

6.6.3.4 BCC a copy of the message

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



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

6.6.3.5 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 route dead letters to a different server (for additional security, since the content could not be scanned).

In the rule action panel, enter a host name or IP address, and a port number, to which MailMarshal should send the message. If you entered a host name, select a protocol to use for delivery (IPv4, IPv6, or either).

MailMarshal uses this address when it attempts delivery, even if the message is passed through.



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.

Copyright © 2026 Trustwave Holdings, Inc.

6.6.3.6 Move the message

This action moves the email message file to the specified folder. Select one of the pre-configured dead letter folders.

This is a terminal action. MailMarshal does not process any further rules for a message if this action is performed.

6.6.3.7 Delete the message

This action deletes the email message file. The message will not be sent to its original destination and will not be available for further review.

When you select this action, you can choose not to create an entry in the MailMarshal SQL logging database for the deleted message. By default MailMarshal logs information about deleted messages so that you can report on the reasons for deletions.



Caution: If you choose not to create a SQL database entry, you will reduce database usage, but you will seriously affect your ability to audit MailMarshal activity. LevelBlue recommends that you create SQL entries.

This is a terminal action. MailMarshal does not process any further rules for a message if this action is performed.

6.6.3.8 Pass message through to recipients

This action allows you to specify that a deadlettered message should be passed through to the original recipient addresses. The destination is subject to the “set message routing to host” action.

6.7 Understanding the Order of Evaluation

The order in which MailMarshal evaluates policy groups and rules can affect the outcome of processing for a message. This is usually due to “terminal” actions that stop MailMarshal processing further rules for a given message.

For instance, by default MailMarshal evaluates virus scanning rules first. If a scanner reports a virus MailMarshal quarantines the message immediately. In this case MailMarshal does not perform any additional processing on the message.

MailMarshal evaluates policy groups and rules in “top down” order as it displays them in the Management Console.

6.7.1 Adjusting the Order of Evaluation of Policy Groups

You can change the order of evaluation by changing the order of the policy group listing in the Management Console.

To adjust the order of evaluation of policy groups:

1. Select a policy type (Connection Policy, Content Analysis Policy, or Dead Letter Policy**)** in the left pane.
2. Select a policy group in the right pane.

Copyright © 2026 Trustwave Holdings, Inc.

3. Move the group up or down using the **Move Up** and **Move Down** buttons above the list.
4. Commit the MailMarshal configuration to effect the change in order.

6.7.2 Adjusting the Order of Evaluation of Rules

You can change the order of evaluation by changing the order of the rule listing in the Management Console.

To adjust the order of evaluation of rules:

1. Expand a policy group.
   - To move a rule up or down within the policy group, use the **Move Up** and **Move Down** buttons above the list.
   - To duplicate a rule within the policy group, right-click and select **Duplicate. T**he duplicate is created at the end of the group.
   - To move or copy rules to another policy group, right-click and select **Copy**. In the Copy window, select the target group(s) and then click **Move** or **Copy**.
2. Commit the MailMarshal configuration to effect the change in order.



Note: MailMarshal always processes Connection Policy before Content Analysis Policy.

If you have configured any rules with “Pass message to rule” or “Move/Copy to folder with release action”, MailMarshal checks for possible processing loops. To prevent problems, MailMarshal will disallow moving the rules, or disable some affected rules.

You can move a referring rule (a rule that includes one of the above actions), subject to the following conditions:

- You cannot move a target rule above a rule that refers to it.
- A rule copied or moved to a policy group above the source is created as disabled. Validation for loops is performed when the rule is enabled.
- If you duplicate a target rule, the original rule remains in place and the duplicate is not a target.

6.8 Viewing Email Policy

You can list the entire email policy or a policy group in a format suitable for printing or copying to a file. For each rule, the listing shows the rule name, a verbose description, and a detailed listing of conditions and actions. The listing also indicates whether the rule is disabled.

To print or copy a listing of the email policy or a policy group:

1. In the left pane of the Management Console, navigate to **Configuration > Email Policy.**
   - To generate a printable view of the entire policy, select the top item in the menu tree (Email Policy). From the menu at the top of the right pane, click **Print**.
   - To generate a printable view of a specific Policy or Policy Group, right-click it in the right pane, and then click **Print** from the context menu.
2. MailMarshal presents the selected items in a print preview window.
3. To print the window contents, click **Print** at the top right. You can also copy part or all of the window contents to the Clipboard using standard Windows commands.

Copyright © 2026 Trustwave Holdings, Inc.

7 Understanding Email Policy Elements

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

Some examples of each type of element are provided by default when MailMarshal is installed. These examples are used in the default email policy.

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

The following types of elements are available:

Connectors

Allow you to import user and group information from Azure Entra, Active Directory or LDAP servers. For more information, see “Configuring Connectors” on page 126.

User Groups

Allow you to apply policy based on email addresses. MailMarshal can retrieve groups from Azure Entra, Active Directory or LDAP servers. You can also create local groups and enter members using wildcard characters.

MailMarshal uses two types of groups: MailMarshal groups and Imported groups. MailMarshal groups contain users and groups that you specify directly. Imported groups contain users and groups that you import from Azure Entra, Microsoft Active Directory servers or LDAP servers. For more information, see “Configuring User Groups” on page 127.

IP Groups

Allow you to apply policy based on the connecting IP address. For more information, see “Configuring IP Groups” on page 129.

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. For more information, see “Identifying Email Text Content Using TextCensor Scripts” on page 130.

Message Templates and Message Stamps

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. For more information, see “Notifying Users with Message Templates and Message Stamps” on page 142.

Copyright © 2026 Trustwave Holdings, Inc.

Virus Scanners

Allow you to check email messages for virus content. For more information, see “Using Virus Scanning” on page 154.

Folders and Classifications

Allow you to quarantine or copy messages, or simply to record the results of MailMarshal evaluation. You can report on folder and classification actions using Marshal Reporting Console. For more information, see “Using Folders and Message Classifications” on page 154.

Email Header Matching and Rewriting

Allow you to search for the content of email header fields using Regular Expressions. You can modify, add, or delete headers. For more information, see “Header Matching and Rewriting” on page 159.

External Commands

Allow you to extend MailMarshal functionality with customized conditions and actions. For more information, see “Extending Functionality Using External Commands” on page 163.

Reputation Services

Allow you to configure settings for externally maintained filtering lists that MailMarshal queries by DNS (also known as DNS Blocklists). For more information, see “Configuring Reputation Services” on page 165.

You can create or edit many policy elements on the fly while you are working with rules. For more information, see “Creating Rules” on page 90. You can also create elements in advance.

To work with policy elements, open the MailMarshal Management Console from the MailMarshal program folder. In the left pane of the Management Console select **Policy Elements.**

7.1 Configuring Connectors

Connectors allow MailMarshal to import user and group information from Azure Entra, Active Directory and LDAP servers. Connectors allow you to import email addresses from user accounts, contacts, groups, and public folders.

For information about creating connectors, see “Creating Directory Connectors” on page 53.

To edit a connector:

1. In the left menu of the Management Interface website, expand **Policy Elements**.
2. In the right pane, click **Connectors**.
3. Select a connector, and then click **Edit**.
4. On the Connector Type tab, you can edit the name and description of the connector.

Copyright © 2026 Trustwave Holdings, Inc.

5. In the Reload Schedule section you can edit the schedule on which MailMarshal checks for updated information on the groups imported through this connector. You can choose to import once a day at a specific time, or more than once a day, or manually.
6. *If this is an Azure Entra connector,* on the Entra Properties tab you can update the tenant, client, and secret.
7. *If this is an Active Directory connector,* on the Active Directory Logon tab you can choose to connect as anonymous, or as a specific account. If you choose to connect using a specific account, enter the account details.
8. *If this is a LDAP connector,* edit the information provided.
    a. On the LDAP Server tab you can edit the server name, port, and logon information. You can choose to connect as anonymous, or as a specific account. If you choose to connect using a specific account, enter the account details. You can enter or browse for a search root for this server. See the Help for full details of the fields on this tab. To change the attributes MailMarshal uses to retrieve group and member information from the LDAP server, click **Advanced.**
    b. On the Group Attributes tab, edit the information MailMarshal will use to retrieve groups from the LDAP server. See the Help for full details of the fields on this tab.
    c. On the User Attributes tab, edit the information MailMarshal will use to retrieve user email addresses from the LDAP server. See the Help for full details of the fields on this tab. For more information about how to retrieve all email addresses from a server, see Knowledgebase article Q11877.

When you have completed all required changes to the connector, click **Save.**

7.2 Configuring User Groups

You can use MailMarshal user groups within policy groups and rules. User groups allow you to apply policy to specific users. MailMarshal uses SMTP email addresses to perform user matching. You can create and populate user groups within MailMarshal by entering email addresses manually or copying them from other Groups. You can use wildcard characters when you define groups. You can also import user groups with the Group File Import tool (see “Using the Group File Import Tool” on page 205).

7.2.1 Creating and Populating User Groups

To create and maintain user groups, in the left pane of the Management Console, select Policy Elements. Then select **User Groups** from the right pane menu.

To create a user group:

1. In the right pane menu of the Management Console, select **User Groups**.
2. From the list header, click **Add**.
3. Enter a name and description for the group.
4. To create the group, click **Save**.

Copyright © 2026 Trustwave Holdings, Inc.

To import a user group:

1. In the right pane menu of the Management Console, select **User Groups**.
2. From the list header, click **Import Connector Group**.
3. To find groups, depending on the connector type click **Browse** or **Search**. Select the desired groups from the results. For more information see Help.
4. To import the selected groups, click **Save**.

7.2.1.1 Adding Members to a MailMarshal Group

You can add addresses or wildcard patterns to a MailMarshal user group.



Note: You can also automatically harvest addresses from email messages into a group. For more information, see “Add message users into group” on page 115.

To add members to a MailMarshal user group:

1. In the left pane of the Management Console, select **Policy Elements**.
2. Select the appropriate user group from the right pane menu or list.
3. From the list heading, click **Add**.
4. On the User Group Member panel, enter an individual SMTP address, a partial address using wildcard characters, or a domain name.



Note: For more information about wildcard characters, see “Wildcard Characters” on page 220.

5. To add the value, click **Save**.
6. Repeat to add more entries.

7.2.1.2 Adding Groups to a MailMarshal Group

You can add Entra, Active Directory, LDAP, and MailMarshal groups to a MailMarshal user group.

To add other groups to a MailMarshal user group:

1. Select a MailMarshal user group from the right pane of the Management Console.
2. From the list heading, click **Add**.
3. Choose **Select a user group**, and then select a group from the list.
4. To add the value, click **Save**.
5. Repeat to add more items.

7.2.1.3 Pruning a MailMarshal Group

You can configure MailMarshal to remove user addresses from a MailMarshal group. You can prune addresses that have not been seen for a time. You can also prune addresses if a group grows too large.

To configure group pruning:

Copyright © 2026 Trustwave Holdings, Inc.

1. Right-click a MailMarshal user group in the right pane of the Management Console, and select **Edit**.
2. Select (toggle on) one or both pruning options (*Delete members who have not been seen* and *Delete members when the group exceeds*), and set the limits.
3. Click **Save.**

For more information about pruning, see Help, and see also Knowledgebase article Q12772.

7.2.2 Moving and Copying Users and Groups

To copy a user group, right-click it in the list in the right pane of the Management Console. To make a copy, choose **Duplicate** from the context menu.

To add a user group to another user group, select the target group and then click **Add**. On the User Group Member panel, choose to select a user group, select a group from the list, and then click **Save**.

To move users or groups, you must delete them from the original location and add them to the new location.

7.3 Configuring IP Groups

You can use MailMarshal IP groups within policy groups and rules. IP groups allow you to apply policy based on the connecting IP address from which an SMTP connection was made or email was received. You can create and populate user groups within MailMarshal by entering individual IP addresses, ranges, or CIDR blocks.

7.3.1 Creating and Populating IP Groups

To create and maintain IP groups, in the left pane of the Management Console, select **Policy Elements**. Then select **IP Groups** from the right pane menu.

To create an IP group:

1. In the right pane menu of the Management Console, select **IP Groups.**
2. From the list header, click **Add**.
3. Enter a name and description for the group.
4. Click **Save**.

7.3.1.1 Adding Members to an IP Group

You can add individual IP addresses, ranges, or CIDR blocks to an IP group.

To add members to an IP group:

1. Select the appropriate user group from the right pane of the Management Console.
2. On the Action menu, select **Insert IPs.**
3. On the Add IP window, complete the required information. See Help for details. When you have completed the information, click **Save.**
4. Repeat these actions to add additional items.

Copyright © 2026 Trustwave Holdings, Inc.

7.3.1.2 Editing an IP Group Member

You can edit the information in an IP Group member record.

To edit a member, double-click the entry in the list, make required changes, and then click **Save**.

7.3.1.3 Adding Groups to an IP Group

You can add other IP groups to a MailMarshal IP group.

To add other groups to a MailMarshal IP group:

1. Select a MailMarshal IP group from the right pane of the Management Console.
2. On the Action menu, select **Insert IP Groups**.
3. In the Insert Into IP Group window, select a group from the list. Click **Save**.
4. Repeat these actions to add additional items.

7.3.2 Moving and Copying IP Groups

To add an IP group to another IP group, in the left pane select it and drag it over the target group in the same pane.

To move entries or groups, you must delete them from the original location and add them to the new location.

7.4 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 Content Analysis Policy rules.

A script can include many conditions. Each condition is based on words or phrases combined using logical and positional 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 Management Console or Marshal Reporting 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.

7.4.1 TextCensor Elements

TextCensor scripts contain one or more expressions, each consisting of a word or phrase.

7.4.1.1 Wildcards

You can use two wildcard characters, anywhere in a word or phrase.

- * matches zero or more letter or digit characters or ideographs.
- ? matches one letter, digit, or ideograph.

Copyright © 2026 Trustwave Holdings, Inc.

Wildcards match only letters and digits, and apostrophes or hyphens that are treated as part of words (see “Word Breaks” on page 134). Wildcards do not match other symbol characters.

Notes:

- You cannot use pure wildcard patterns comprised entirely of a mixture of `[DIGIT]`, `[LETTER]`, `*`, or `?`
- Make patterns as specific as possible. Patterns that produce a very large number of matches will take a long time to evaluate and consume unacceptable amounts of system resource. For example, do not use the patterns `*e*` or `a*` when evaluating English-language documents.

If you want to set the order of evaluation of a complex expression that uses more than one operator, use parentheses ( ).

Each TextCensor expression can include logical and positional operators. The operators must be entered in UPPERCASE.

7.4.1.2 Positional Operators

TextCensor works with the positions of words or phrases within a file. For example, in the sentence “The quick brown fox jumps over the lazy dog” the word “quick” starts and ends at position 2, and the phrase “jumps over” starts at position 5 and ends at position 6.

A positional operator works with expressions that evaluate to sets of positions. It takes two sets of positions as parameters, and returns a new set of positions.

Tip: In a simple TextCensor expression, you can think of the expression result as “true” or “matched” if the word or phrase is found in any position in the text. When the word or phrase is found in more than one position, this counts as more than one match of the expression.

When you combine positional operators to make a complex expression, note the explanations of the sets returned by each operator (see below). Test your script before applying it in production.

You can specify a distance for many positional operators. The default distance (if you do not specify a value) is 4.

Table 14: TextCensor Positional Operators

Operator and Syntax	Matching Results
FOLLOWEDBY `A FOLLOWEDBY[=distance] B`	The start of B occurs within *distance* words from the end of A. Returns a set of positions spanning from the start of A to the end of B. `dog FOLLOWEDBY hous*` matches `Dog in the house`
NOT FOLLOWEDBY `A NOT FOLLOWEDBY[=distance] B`	The start of B does not occur within *distance* words from the end of A. Returns a set containing the positions in A that are not followed by B. `dog NOT FOLLOWEDBY=1 hous*` matches `Dog in the house`

Copyright © 2026 Trustwave Holdings, Inc.

Table 14: TextCensor Positional Operators

Operator and Syntax	Matching Results
PRECEDEDBY `A PRECEDEDBY[=distance] B`	The end of B occurs within *distance* words from the start of A. Returns a set of positions spanning from the start of B to the end of A. `dog PRECEDEDBY cat` matches `Cat chasing dog`
NOT PRECEDEDBY `A NOT PRECEDEDBY[=distance] B`	The end of B does not occur within *distance* words from the start of A. Returns a set containing the positions in A that are not preceded by B. `dog NOT PRECEDEDBY=2 cat` matches `Cat was not chasing dog`
NEAR `A NEAR[=distance] B`	If A occurs within *distance* words before B the resulting position spans from the start of A to the end of B. If B occurs within *distance* words before A the resulting position spans from the start of B to the end of A. `dog NEAR cat` matches `Cat chasing dog` and also matches `Dog chasing cat`
NOT NEAR `A NOT NEAR[=distance] B`	Returns the positions of all instances of A where B is not found within *distance* words from A `dog NOT NEAR=2 cat` matches `Cat was not chasing dog` and also matches `Dog was not chasing cat`
OR `A OR B`	This form of the OR operator is applied when both A and B are sets of positions, even if one or both are empty sets. It returns the union of position sets A and B. For the sentence "A rose is a rose", the expression `(rose OR is)` returns the position set 2,3,5.

7.4.1.3 Logical (Boolean) and Special Operators

A logical operator takes Boolean (true/false) values as input, and returns a Boolean result. These results cannot be used as parameters of a positional operator.

When one of the parameters to a logical operator is an expression that returns a position set, the parameter is treated as a logical value. A set with at least one position match is treated as true. A set that has no matches is treated as false.

TextCensor also supports the special operator INSTANCES.

Table 15: TextCensor Logical and Special Operators

Operator and Syntax	Matching Results
OR `A OR B`	Returns true if A or B (or both) is true. This form of the OR operator is applied when either A or B (or both) are logical expressions. If both A and B are position sets then the positional OR operator is used instead.

Copyright © 2026 Trustwave Holdings, Inc.

Table 15: TextCensor Logical and Special Operators

Operator and Syntax	Matching Results
AND `A AND B`	Returns true if both A and B are true.
NOT `NOT A`	Returns the opposite of A (true if A is false).
INSTANCES `A INSTANCES=count`	A must be an expression that returns a position set. The result is true if A contains *count* or more word positions; otherwise the result is false.

7.4.1.4 Anchored Regular Expressions

TextCensor supports use of Regular Expressions through the ARX operator.

An anchored regular expression is a regular expression (regex) which must be preceded by a word on the left hand side of the ARX operator. Matching of the regex begins at the next character following the word. Regex patterns should always begin by matching one or more non-word characters. In most cases you can start the regex pattern with \W (to match whitespace).

Notes:

- ARX is based on Google RE2. The syntax is generally similar to the syntax used in MailMarshal Header Matching (see “Regular Expressions” on page 221).
- Distance parameters for ARX operators are specified in characters. The default is 100 characters.
- Regular expressions are case insensitive by default. You can force case sensitive matching with the operator `?-i`
- ARX does not support lookahead or lookbehind.
- ARX does not support capture groups. Capture groups will be ignored or converted to non-capturing sequences.
- ARX does not support `\Q...\E` literal text.
- For further details of the ARX syntax, see the RE2 wiki.

Table 16: TextCensor Regular Expression Operators

Operator and Syntax	Matching Results
ARX `A ARX[=distance] /pattern/`	Locates instances of A where it is followed by text matching the regex pattern within *distance* characters of the end of A. The entire pattern must occur within the specified distance. The resulting position list spans from the beginning of A to any content matched by the regex. `dog chasing ARX /\W(one|two|10) cat(s*)/`
NOT ARX `A NOT ARX[=distance] /pattern/`	Locates instances of A where text matching the regex pattern does not occur within *distance* characters of the end of A. When this expression matches, the resulting position list is the position list of A.

Copyright © 2026 Trustwave Holdings, Inc.

Multiple anchored regular expressions can be combined with other expressions and operators to create complex statements. For example,

```
((dog OR boy) FOLLOWEDBY=1 ((chasing OR leading) ARX /\W(one|two|10)/) NEAR
big) FOLLOWEDBY (white ARX /\W(horse|cat)s*/)
```

matches the phrase: *dog chasing one or more big white cats.*

7.4.2 TextCensor Concepts

The following concepts clarify how TextCensor expressions are evaluated.

Note: This section does not apply to Regular Expression patterns.

7.4.2.1 Words

A word is made up of one or more letters and digits, and sometimes symbols.

- In alphabetic languages, a word is a group of letters or digits separated by other characters (such as punctuation, other symbols, and white space).
- In Chinese, or Japanese kanji, a word or “token” may be composed of one or more characters (ideographs).

7.4.2.2 Phrases

A phrase is made up of a series of words separated by word break characters.

7.4.2.3 Symbols and Punctuation

Symbols other than letters and digits are not treated as part of a word unless they appear in the specific statement being evaluated. A group of symbols is not treated as a word.

Tip:

- The text `word$deed` is matched as two words by the expression `word FOLLOWEDBY deed`, and also by the exact expression `word$deed`
- The text `$word$` is matched by any of `word`, `$word`, `word$`, or `$word$`
- The text `Save $$$ Now` is matched by `save FOLLOWEDBY=1 now`

7.4.2.4 Word Breaks

The sets of characters that are treated as word and number break characters generally follow Unicode standards.

Copyright © 2026 Trustwave Holdings, Inc.

A word break character can also be matched exactly or by a wildcard.

Tip:

- Each of the following strings is treated as one word:
  `John's`
  `3.14159`
  `1,234.56`
  `3a`
  `REV.B` (the full stop between letters with no surrounding spaces is not a word break)
- The text `half-baked` is treated as two words and is matched by any of the following expressions:
  `half FOLLOWEDBY=1 baked`
  `half-baked`
  `half?baked`

7.4.2.5 Accented Letters

TextCensor treats each accented character as a single letter. A letter with additional composed accent characters is normalized to a single character before the text is evaluated.

7.4.2.6 Escape Characters

Some characters have special meanings in TextCensor. These characters are parentheses, square braces, the asterisk, the equal sign, the double quote character, and the question mark. You can place a backslash character ('\') before any of these characters in order to use the character's normal meaning. To use a normal backslash character, place two of them together ("\\").

Within ARX expressions, the Regular Expression reserved characters apply (in particular the forward slash '/') which marks the start and end of the regex pattern).

7.4.2.7 Case Sensitivity

TextCensor evaluation is NOT case sensitive by default. To perform a case sensitive match, quote the content using double quote characters. All special characters and escape characters retain their meaning within double quotes.

7.4.2.8 Classes

You can use TextCensor Classes to match specific types of characters inside a word, or special types of words.

Table 17: TextCensor Classes

Operator and Syntax	Matching Results
[LETTER]	Matches any single letter inside a word.
[DIGIT]	Matches any single digit inside a word. For example, `A[LETTER]B[DIGIT]C` would match both "axb0c" and "aab9c".

Copyright © 2026 Trustwave Holdings, Inc.

Table 17: TextCensor Classes

Operator and Syntax	Matching Results
[NUM]	Use in place of a word to match any number made up of one or more digits. This class does not match numbers with a decimal point, or Asian language numbers that use words between characters
[CCARD]	Use in place of a word to match a series of digits that look like credit/payment card numbers. These numbers consist of up to 5 groups of digits, are up to 19 digits in length, and must pass checksum validation (using the Luhn algorithm). This class should match most card numbers.
[US-SSN]	Use in place of a word to match series of digits that look like US Social Security Numbers. Valid numbers must follow a specific format. However, the format is loosely defined and it is not possible to prevent accidental matching of other numbers.
[CAN-SIN]	Use in place of a word to match a series of digits that looks like a Canadian Social Insurance Number. Valid numbers must follow a specific format and pass a Luhn check.

7.4.2.9 Named Statements

You can give a TextCensor statement a name. When a named statement is executed, the result is stored. You can reference it in later statements within the same script.

If a statement contains only words or only uses positional operators, the stored result is the set of word positions found by that statement. If the statement uses any other operators then the result is logical.

You can reference the result of a statement by using `[@name]` inside a statement. This can be used anywhere that you would otherwise use the bracketed result of an operator.

Note: Naming a statement does not affect the statement's score. To use a named statement as a macro expression, in most cases you should set the statement's score to zero.

When using named statements within other expressions, remember that the result must match the required parameter type. If a statement returns a logical result you cannot use it as a parameter to a positional operator. Test your scripts before applying them in production.

7.4.3 Scoring a TextCensor Script

Each script is given a trigger threshold, expressed as a number. Each expression in a script is given a positive or negative score. If the total score of the content being checked reaches or exceeds the trigger threshold, the script is triggered.

The total score is determined by summing the scores resulting from evaluation of the individual expressions in the script.

For each expression, if the result is a true logical value, the expression score is the base score.

Copyright © 2026 Trustwave Holdings, Inc.

If the expression result is a position set (the word or phrase was found one or more times in the text), by default the final score of the expression is the base score. You can choose how to add the score when the expression is matched more than once. The options are:

Table 18: Cumulative scoring options

Option	Description
Every time	Each match of the words or phrases adds the score to the total.
First Match Only	Only the first match of the words or phrases adds the score to the total.
First N Matches	Each match, up to the number you set, adds the score to the total. For instance if the expression score is 5 and you select “first 3 matches,” then the expression can contribute up to 15 to the total score, but never more than 15.

Negative scores and trigger levels allow you to compensate for the number of times a word could be used in text that you do not want to match. For instance: if `breast` is given a positive score in an “offensive words” script, `cancer` could be assigned a negative score (since the presence of this word suggests the use of `breast` is medical/descriptive).



Note: Script evaluation always checks all expressions to obtain the final score. The order of expressions in a script is not significant. This is a change from earlier versions.

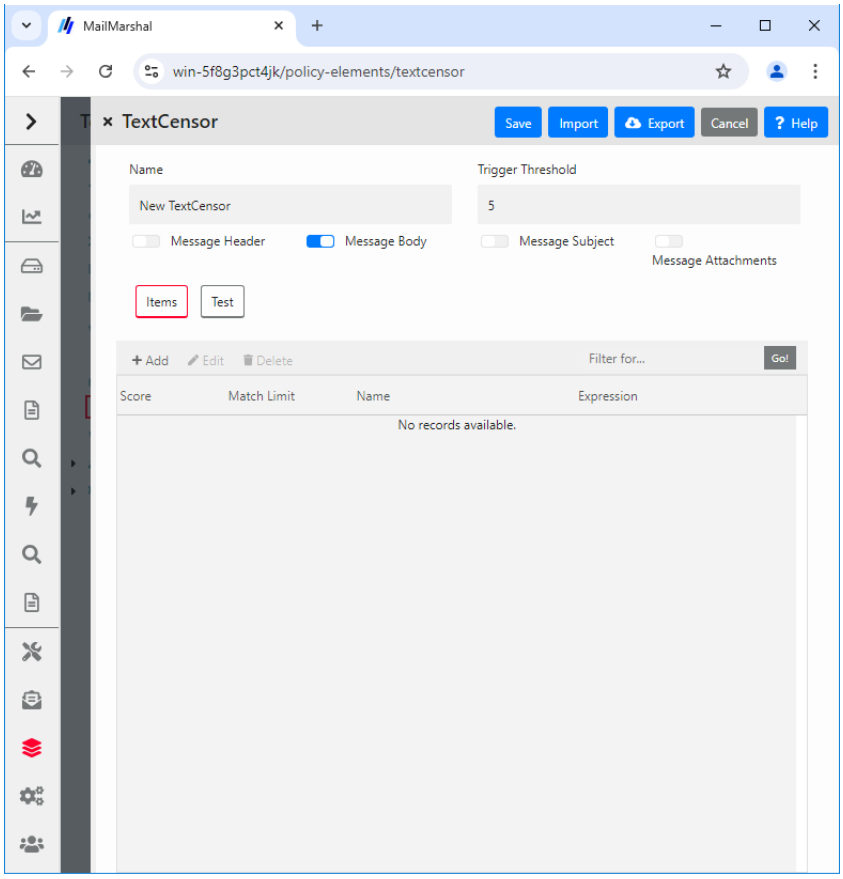
7.4.4 Creating Scripts

To work with TextCensor Scripts, in the left pane of the Management Console, select **Policy Elements**. Then select **TextCensor Scripts** from the right pane menu.

To add a TextCensor Script:

1. In the right pane of the Management Console, select **TextCensor Scripts.**
2. On the menu above the list, choose **Add** to open the TextCensor Script window**.**

Copyright © 2026 Trustwave Holdings, Inc.



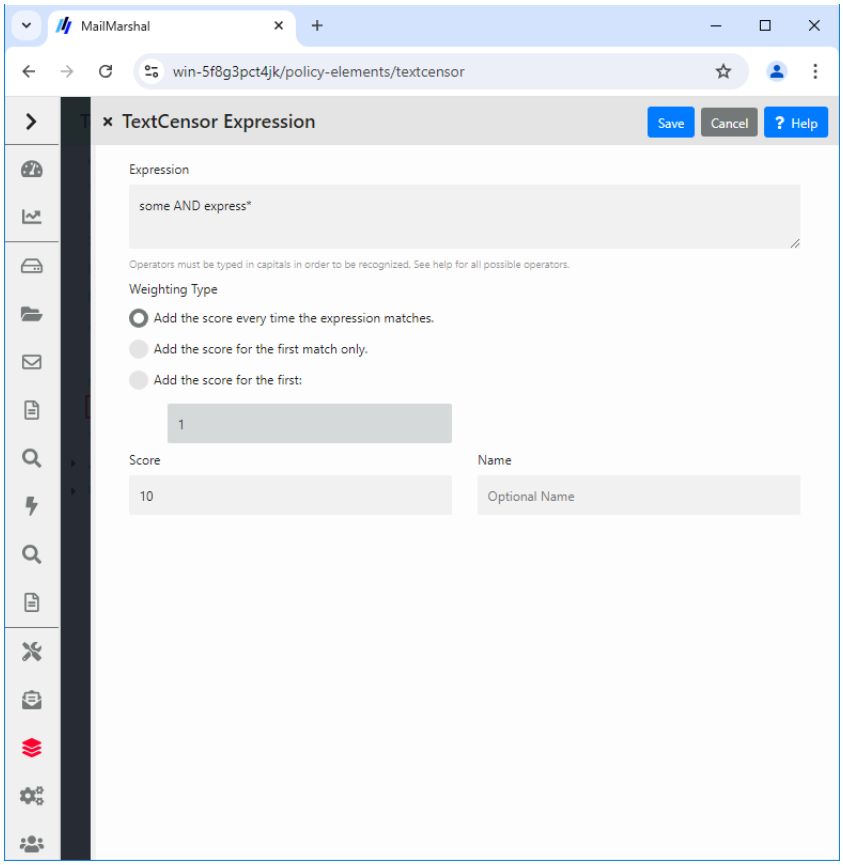
3. Enter a name for the script.
4. Select which portions of an email message you want this script to scan by selecting one or more of the check boxes Subject, Headers, Body, and Attachments

Note: The script will check each part separately.

For instance, if you select both Headers and Message Body, the script will be evaluated once for the headers, then again for the body. Script scoring is not cumulative over the parts.

5. Add one or more TextCensor items. To begin adding items, in the TextCensor Script window click **New** to open the Add TextCensor expression window**.**

Copyright © 2026 Trustwave Holdings, Inc.



6. Enter the expression, optionally using the operators described earlier. For example:

   ```
   (Dog FOLLOWEDBY hous*) AND NOT cat
   ```

   In this example the expression score is added to the script total if the document contains the words `dog house` (or `dog houses`, and so forth) in order, and does not contain the word `cat`.



Note: TextCensor expressions are **not** case sensitive by default. However, quoted content is case sensitive. So `textcensor` would match TextCensor, but "`textcensor`" would not.

7. Select a score and contribution method for this expression (see "Scoring a TextCensor Script" on page 136 for more information).
8. Click **Add** (or press **Enter**) to add the expression to this script. The window remains open so you can create additional expressions.
9. When you have finished entering expressions, click **Close** to return to the New TextCensor Script window.
10. Select a trigger threshold. If the total score of the script reaches or exceeds this level, the script is triggered. The total score is determined by evaluation of all expressions in the script.

7.4.5 Editing Scripts

You can change the content of an existing script, including the individual items and overall properties.

To edit a TextCensor Script:

Copyright © 2026 Trustwave Holdings, Inc.

1. Double-click the script to be edited in the right pane.
2. Edit an item by double-clicking it.
3. Delete an item by selecting it, and then clicking **Delete.**
4. Change the contents of other fields such as the script name, parts of the message tested, and trigger threshold.
5. Click **Save** to accept changes or **Cancel** to revert to the stored script.

7.4.6 Duplicating Scripts

Duplicate a script if you want to use it as the basis for an additional script.

To duplicate a TextCensor Script:

1. Right-click the script name in the Management Console.
2. Choose **Duplicate** from the context menu.
3. After duplicating the script, make changes to the copy.

7.4.7 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: Some older product versions used a different format for the exported scripts. The earlier version scripts will be upgraded to the new format automatically. Any problems with upgrading will be reported.

To import a TextCensor Script from an XML file:

1. On the Action menu, choose **New TextCensor Script** to open the TextCensor Script window**.**
2. Click **Import**.
3. Choose the file to import from, and click **Open.**
4. In the Edit TextCensor Script window, click **Save**.

7.4.8 Exporting Scripts

You can save scripts in files. Use this function to move a script between MailMarshal installations, 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 open the Edit TextCensor Script window.
2. Click **Export.**
3. Enter the name of the file to export to, and click **Save**.
4. In the Edit TextCensor Script window, click **Save.**

Copyright © 2026 Trustwave Holdings, Inc.

7.4.9 TextCensor Best Practices

To use TextCensor scripts effectively, you should understand how the TextCensor facility works and what it does.

MailMarshal applies TextCensor scripts to text portions of messages. Depending on the portions you select, a script can apply to message subject, message 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.



Note: When you apply complex scripts to large documents, the script evaluation can consume significant system resources and process slowly. Use the minimum number of statements and operators, and match the most specific text possible.

7.4.9.1 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 score. For instance, if your organizational Acceptable Use Policy lists specific terms that are unacceptable, you should give those terms a higher score 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.

7.4.9.2 Decreasing Unwanted Triggering

TextCensor scripts sometimes trigger on message content which is not obviously related to the content types they are intended to match.

To troubleshoot unwanted triggering:

1. Use the problem script in a rule which copies messages and their processing logs to a folder. You could call this folder “suspected sports messages”.
2. After using this rule for some time, check on the messages that have triggered the script. Review the message logs to determine exactly which words caused the script to trigger. See “Viewing Messages” on page 170.
3. Revise the script by changing the expression scores, expression contribution method, trigger threshold, or key words, so as to trigger only on the intended messages.

Copyright © 2026 Trustwave Holdings, Inc.

4. When you are satisfied, modify the rule so as to block messages that trigger the script. You could also choose to notify the sender and/or the intended recipient.

7.4.10 Testing Scripts

When you are working with a TextCensor script in the Management Console, you can test it against a file or pasted text.

To test a TextCensor Script:

1. On the New or Edit TextCensor Script window, click **Test**.
2. *To test using a file,* select **Test script against file.** Enter the name of a file containing the test text (or browse using the button provided).
3. *To test using pasted text,* select **Test script against text**. Type or paste the text to be tested in the field.
4. Click **Test.** MailMarshal will show the result of the test, including details of the items which triggered and their weights, in the **Test Results** pane.

7.5 Notifying Users with Message Templates and Message Stamps

MailMarshal 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 can use special digest templates to provide users with summary information about quarantined email.

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.

7.5.1 Message 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.

Copyright © 2026 Trustwave Holdings, Inc.

You can also use a notification to set up a general auto responder based on message headers or content. For instance, MailMarshal could respond to a message to `robot@ourcompany.com` with the subject “Send Catalog” by returning the product catalog to the sender as an email attachment.

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



Note: In addition to rule notification templates, MailMarshal uses a number of pre-configured templates for administrative notifications (such as delivery failure notifications). For more information about modifying these templates, see “MailMarshal Properties – Advanced” on page 200.

7.5.2 Creating a Message Template

To work with templates, in the left pane of the Management Console, select **Policy Elements**. Then select **Message Templates** from the right pane menu.

To create a message template:

1. In the right pane of the Management Console, select **Message Templates.**
2. On the Action menu, select **New Message Template** to open the Message Template window.
3. By default, MailMarshal creates a HTML message body. MailMarshal will automatically generate a plain text equivalent of the message body when using the template. To choose a plain text body or edit both types separately, click **Options.**
4. To see additional address fields, click **Options.**
5. Enter a name for the template.
6. Enter appropriate information in the Header Details section. For instance, enter the email address to which replies should be sent in the **Return Path** field.



Note: The MailMarshal default configuration includes numerous templates. These are a good source of ideas for the creation of new templates.

7. Enter text in the body section. To view the raw HTML, right-click in the HTML pane and select **Edit Raw HTML.** Edit the HTML, or paste HTML source from another editor, then click **Save** to return to the message template window.
8. You can attach files to the notification, including the original message, the MailMarshal message processing log, and other files. To attach one or more files, select the appropriate box(es) and enter the file names if necessary.

Copyright © 2026 Trustwave Holdings, Inc.

9. You can use variables marked with braces { }. To see a list of variables available in any field, type { to open a context menu. You can also enter variable names manually. You can use nested variables. For details of the variables available in templates, see “Using Variables” on page 148.



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.

7.5.3 Creating Digest Templates

The MailMarshal 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 213.

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

- You cannot attach files to digest templates.
- You must associate each digest template with a message digest. See “Setting Up Message Digests” on page 213.
- You cannot edit the “To” field. The recipient is controlled by settings of the 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.

Table 19: Digest detail levels

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.

Table 20: Digest options

Option	Results
SHOWRELEASE	Show the message release link for each message (default option).

Copyright © 2026 Trustwave Holdings, Inc.

Table 20: Digest options

Option	Results
RELEASETRUST	For incoming digests, in addition to the release link, show a “Trust” link for each message (in the Sender column). If the “Trust” link is clicked, release the message and also add the sender to the user’s Safe Senders list. • For the Trust feature to function, SQM must be configured, and user management of safe senders must be enabled (in the Administrator tab of the SQM site). • With SQM Forms authentication, if the digest recipient’s address is not found as a SQM user or alias, MailMarshal creates a SQM user and sends a password email. With SQM Windows authentication, the address must pre-exist as an alias.
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 of the local MailMarshal Spam Quarantine Management website. A URL could be specified, for instance, in the digests for user groups that cannot browse to the default location.
GROUP	Group entries by folder, for digests covering multiple folders.
SHOWFROM=*yes|no*	Show the sender address. Defaults to yes.
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/SpamConsole}
```

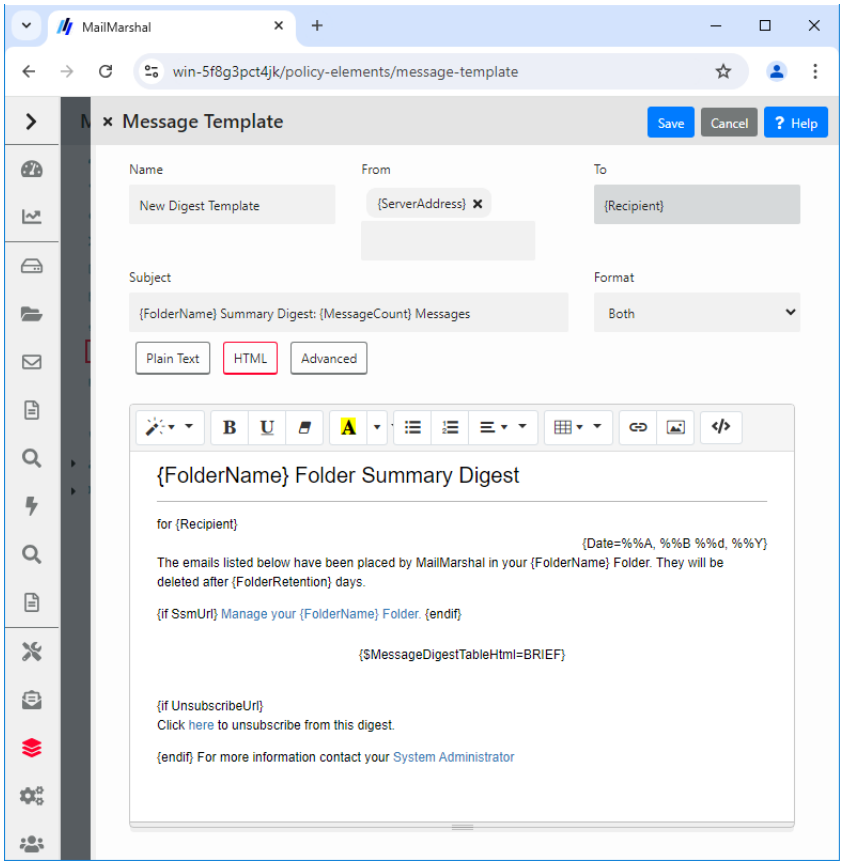
For details of other variables available in digest templates, see “Using Variables” on page 148.

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 right pane of the Management Console, select **Message Templates.**
2. On the Action menu, select **Add Digest** to open the Digest Template window.

Copyright © 2026 Trustwave Holdings, Inc.



3. By default, MailMarshal populates the template with basic information. MailMarshal creates separate HTML and plain text message bodies. To choose to use only one of the two types, click **Options.**
4. To see additional address fields, click **Options.**
5. Enter a name for the template.
6. Enter appropriate information in the Header Details section. For instance, enter the email address to which replies should be sent in the **Return Path** field.
7. Enter text in the body section. To view the raw HTML, right-click in the HTML pane and select **Edit Raw HTML.** Edit the HTML, or paste HTML source from another editor, then click **Save** to return to the message template window.
8. You can use variables marked with braces { }. To see a list of variables available in any field, type { to open a context menu. You can also enter variable names manually. You can use nested variables. For details of the variables available in templates, see “Using Variables” on page 148.
9. Click **Save.**

7.5.4 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 Management Console.

Copyright © 2026 Trustwave Holdings, Inc.

2. Make changes then click **Save.** If you have created both a plain text and a HTML version of the template, remember to change both versions.

7.5.5 Duplicating Templates

You can make a copy of a template if you want to use it as the starting point for another template.

To copy a template:

1. Right-click a template name in the Management Console.
2. Choose **Duplicate** from the context menu.
3. After duplicating the template, make changes to the copy.

7.5.6 Deleting Templates

You can delete a template if it is not used in any rules.

To delete a template:

1. Select a template in the Management Console.
2. Click the **Delete** icon in the toolbar.

7.5.7 Working 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 left pane of the Management Console, select **Policy Elements**. Then select **Message Stamps** from the right pane menu.

To create a message stamp:

1. In the right pane of the Management Console, select **Message Stamps.**
2. On the Action menu, select **New Message Stamp**.
3. Enter a name for the stamp.
4. Select whether the stamp is to appear at the top or the bottom of messages.
5. Enter a plain text version of the message stamp in the Plain Text tab.
6. Enter an HTML version of the stamp in the HTML tab.
    - You can apply various formatting, including hyperlinks, to the HTML text using the buttons provided.
    - You can define and use local CSS classes in a stamp. See Help for details.

Copyright © 2026 Trustwave Holdings, Inc.

- To view the raw HTML, right-click in the HTML pane and select **Edit Raw HTML.** Edit the HTML, or paste HTML source from another editor, then click **Save** to return to the message stamp window.

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



Note: If message stamping is enabled for RTF (Microsoft TNEF) messages, the plain text message stamp will be used for these messages. To enable RTF stamping, see the Engine Advanced section of MailMarshal Properties.

Both plain text and HTML message stamps can include the same variables available within email notification templates.

7.5.7.1 Duplicating Message Stamps

You can make a copy of a stamp if you want to use it as the starting point for another stamp.

To duplicate a message stamp:

1. Right-click the stamp name in the Management Console.
2. Choose Duplicate from the context menu.
3. After duplicating the message stamp, make any required changes to the copy. Remember to make changes to both the Plain Text stamp and the HTML stamp.

7.5.7.2 Editing Message Stamps

You can make changes to a stamp. Remember to make changes to both the Plain Text stamp and the HTML stamp.

To edit a message stamp:

1. Double-click the stamp name in the right hand pane of the Management Console.
2. Make the required changes.
3. Click **Save.**

7.5.7.3 Deleting Message Stamps

You can delete a message stamp if it is not used in any rules.

To delete a message stamp:

1. Select the stamp in the right hand pane of the Management Console.
2. Click the **Delete** icon in the toolbar.

7.5.8 Using Variables

You can use variables when you create a message template, digest template, message stamp, or message classification description, and also in the field substitution of content analysis Header Rewrite rules. MailMarshal substitutes the appropriate information when processing each message or digest.

Copyright © 2026 Trustwave Holdings, Inc.

Variables are marked by curly braces { }. You can select from available variables in any field where they are available in a template, stamp, or classification. To see a list of available variables in a specific field, type { .

Not all variables are available in all contexts. MailMarshal may not have the required information to substitute. In particular, if a message is deadlettered, information about the message content is not available. If MailMarshal does not have any data, it will enter empty text into the variable marker or return the variable marker text.

The following table lists commonly used variables and their functions:

Table 21: MailMarshal variables

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 144. See also the variable {MessageDigestTableText}.
{Administrator}	Email address of the administrator as set during post-installation configuration and accessible from the Notifications section of MailMarshal Properties.
{ArrivalTime}	The time when MailMarshal received a message.
{AttachmentName}	File name of the attached file that triggered a rule condition.
{CmdFileName}	Full path to a file unpacked from the message being scanned. Used in the parameters of an External Command or Command Line Virus Scanner to take action on a specific file.
{Date}	The current date. For more information, see “Date Formatting” on page 153.
{DateLastRun}	The date of the previous MailMarshal message digest for a folder.
{Errorlevel}	The last error returned by a virus scanner or an external command.
{ExternalCommand}	The name of the last External Command used.
{Env=*varname*}	Inserts the value of a Windows environment variable.
{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.
{FolderRetention}	The retention period for a folder that is the subject of a MailMarshal message digest email.

Copyright © 2026 Trustwave Holdings, Inc.

Table 21: MailMarshal variables

Variable	Data inserted
{FormattedRecipients}	Available in Engine dead letter templates only. Lists recipients of the message (in the To: or CC: fields), formatted for use in the message body.
{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, formatted for use in the message body.
{From}	Email address in the 'From' field of the message.
{HasAttachments}	Returns '1' if the message has attachments.
{Header-Reply-To}	Email address in the 'Reply-To' header of the email message. If the 'Reply-To' header is not present, the return-path email address is used.
{HelloName}	Name given by the remote email server when MailMarshal received this message.
{Hostname}	The host name of the server.
{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.
{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, CC and BCC recipients. • To preserve the privacy of BCC recipients when sending notifications, do not use this variable in the template TO: field or in the body of the template. Place this variable in the BCC: field.
{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.

Copyright © 2026 Trustwave Holdings, Inc.

Table 21: MailMarshal variables

Variable	Data inserted
{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.
{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 215.
{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 215.
{RemoteDomainName}	The name of the domain on the remote machine (connecting email server).
{RemoteIP}	The IP of the remote machine.
{ReplyTo}	SMTP “Mail From” email address.
{ReputationServices}	A list of Reputation Services (DNS blocklists) that triggered on the message within a Connection Policy 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 SMTP “Mail From” email 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).

Copyright © 2026 Trustwave Holdings, Inc.

Table 21: MailMarshal variables

Variable	Data inserted
{SenderIDScope}	The scope of the Sender ID check (`pra` or `mfrom`).
{SenderIP}	IP address of the sender.
{ServerAddress}	Email address used as the 'From' address for notifications as set during post-installation configuration and accessible from the Notifications section of MailMarshal Properties.
{SpamBotCensorResult}	The result string as returned by the SpamBotCensor facility.
{SpamBotCensorScore}	The numeric score as returned by the SpamBotCensor facility.
{SpamCategoryResult}	The result string as returned by a Category script rule condition (other than SpamCensor or SpamBotCensor). If you run more than one Category condition on a message, this variable returns only the result of the latest condition (at the time the variable is used).
{SpamCategoryScore}	The numeric score as returned by the latest Category script rule condition (other than SpamCensor or SpamBotCensor). If you run more than one Category condition on a message, this variable returns only the score of the latest condition (at the time the variable is used).
{SpamCensorResult}	The result string as returned by the SpamCensor facility.
{SpamCensorScore}	The numeric score 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 MailMarshal Spam Quarantine Management Website. You can change this value on the Administrator tab of the SQM website.
{StrippedFiles}	The names of any attachment files stripped from the message by rule action.
{Subject}	Message subject, decoded if applicable. Use this variable in most cases. See also {RawSubject}.
{ThreadWorking}	The MailMarshal working folder name.
{Time}	The current time. See also “Date Formatting” on page 153.
{TimeEnteredQueue}	The time that the message entered the MailMarshal Queue.
{TimeLeft}	The time left to attempt delivering the message in question.
{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}`

Copyright © 2026 Trustwave Holdings, Inc.

Table 21: MailMarshal variables

Variable	Data inserted
{VirusName}	Name of the virus detected. This information is only available if the virus scanner being used is a DLL based scanner. If a command line scanner reports a virus this variable is set to “Unknown.”
{VirusScanner}	Name of the virus scanner used.

7.5.9 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}.

To use locale-specific settings you must ensure that the Windows locale is applied to the account used by MailMarshal services. For more information, see Knowledgebase article Q12670.

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

Table 22: Date formatting variables

Variable	Value inserted
a	Abbreviated weekday name
A	Full weekday name
b	Abbreviated month name
B	Full month name
c	Date and time representation appropriate for locale
d	Day of month as decimal number (01–31)
H	Hour in 24-hour format (00–23)
I	Hour in 12-hour format (01–12)
j	Day of year as decimal number (001–366)
m	Month as decimal number (01–12)
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)

Copyright © 2026 Trustwave Holdings, Inc.

Table 22: Date formatting variables

Variable	Value inserted
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

7.6 Using Virus Scanning

You can implement virus/malware scanning as an email policy element. For more information, see “Stopping Viruses and Malware” on page 75.

7.7 Using Folders and Message Classifications

MailMarshal uses a Microsoft SQL Server database to log basic information about each message it has processed. This information includes the sender, recipient, message size, and actions taken.

If MailMarshal moves or copies a message to a folder, it logs this event in the database.

Using Message Classifications is another way to add detail to the log records. You can add Message Classifications by including an action within a MailMarshal Content Analysis Policy rule. You can view the classification given to a particular message using the Console Message History or reports from Marshal Reporting Console.

You should include at least one logging action (either a folder action or a Classification action) in each Content Analysis Policy rule. MailMarshal default rules include such actions.

Note: To avoid confusion in reporting, MailMarshal will not allow a folder and a classification with the same name.

7.7.1 Working with Message Classifications

Message Classifications are useful for reporting on broad categories, such as viruses or executable files quarantined. You can also use classifications to record very specific occurrences such as a specific file or size of file being sent. For example you could answer the question “How many PDF files over 500K in size are sent by Sales each week?” by creating a rule to log sending of such files. If several rules place messages in a single MailMarshal folder, you can use classifications to give additional granularity for searching and reporting.

To work with classifications, in the left pane of the Management Console, select **Policy Elements**. Then select **Classifications** from the right pane menu. To create a message classification:

Copyright © 2026 Trustwave Holdings, Inc.

1. On the menu above the list, choose **Add.**
2. In the window, enter a meaningful name for the classification.
3. Give a brief description of the classification and its purpose. This description will be used in the Console and Reports, and can contain { } variables as in message stamps and templates.
4. To add the classification, click **Save**.

7.7.1.1 Editing Message Classifications

You can edit the name and description of a classification.

To edit a message classification:

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

7.7.1.2 Duplicating Message Classifications

You can make a copy of a classification if you want to use it as the starting point for another classification.

To duplicate a message classification:

1. Right-click the classification name in the Management Console.
2. Choose **Duplicate** from the context menu.
3. After duplicating the classification, make any required changes to the copy.

7.7.1.3 Deleting Message Classifications

You can delete a classification if it is not used in any rules.

To delete a message classification:

1. Select the classification name in the right pane of the Management Console.
2. Click the **Delete** icon in the toolbar.

7.7.2 Working with 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.

MailMarshal also uses special “Dead Letter” folders to store messages that it could not completely process. You can manage messages in these folders in many of the same ways that you can manage quarantined messages.

Copyright © 2026 Trustwave Holdings, Inc.

You can configure folders with specific security settings. You can configure folders to be available for end-user management through the Spam Quarantine Management console. You can configure folders to allow “fingerprinting” of released messages.



Note: In earlier versions of MailMarshal you could configure the default action that MailMarshal took if a message was released from a folder. This option has been replaced by the “release action” option in rule actions. For more information, see “Copy the message” on page 114 and “BCC a copy of the message” on page 117.

MailMarshal includes predefined folders that address common email security issues and automatically categorize quarantined mail. MailMarshal provides many predefined folder types, including folders that:

- Hold messages quarantined due to rule action (for instance, messages that are categorized as spam, virus infected, contain disallowed attachments, or blocked for other policy reasons).
- Hold archived messages.
- Hold historical information about delivered messages (Sent History).
- Hold messages that MailMarshal cannot process or cannot deliver, called dead letters. Dead Letters can result from bad email addresses, from corrupted data, from differing interpretations of Internet standards, or when a message is intentionally malformed in an attempt to exploit a security vulnerability.

Predefined and newly-created folders have default properties that you can modify. For example you can specify a custom file system location for a folder.

If existing MailMarshal folders are not appropriate for your needs, modify the properties of an existing folder or create your own folders.

7.7.3 Creating Folders

You can create as many folders as your policy requires. You can create the following types of folders:

Standard Folder

Used to quarantine dangerous or suspect mail. You can specify that an administrator or regular user can manage the folder contents through SQM. You can specify that messages released from the folder are eligible for attachment fingerprinting.

Archive Folder

Used to keep historic copies of delivered mail. MailMarshal saves messages stored in the folder for a specific period of time. You cannot manually delete mail stored in an archive folder. You can specify that messages released from the folder are eligible for attachment fingerprinting.

Parking Folder

Used to delay the delivery of mail. MailMarshal releases messages stored in the folder according to a predefined schedule.

To create a folder:

Copyright © 2026 Trustwave Holdings, Inc.

1. In the left pane of the Management Console, select **Policy Elements**. Then select **Folders** from the right pane menu.
2. On the menu above the list, click **Add.**
3. Specify the appropriate values. For more information about available settings, click **Help**.
4. Click **Save.**

7.7.4 Editing Folders

You can change the name and most features of a folder. You cannot change the type of an existing folder. You cannot change the name of dead letter folders.

To edit a folder:

1. In the left pane of the Management Console, select **Policy Elements**. Then select **Folders** from the right pane menu.
2. Double-click the folder you want to modify.
3. Specify the appropriate values. For more information about available settings, click **Help**.
4. Click **Save**.

7.7.4.1 Deleting Folders

You can delete a folder if it is not used in any rules. You cannot delete dead letter folders.

To delete a folder:

1. In the left pane of the Management Console, select **Policy Elements**. Then select **Folders** from the right pane menu.
2. Click the **Delete** icon on the menu above the list.

Deleting a folder in the Management Console deletes only the link to the folder that appears in the Management Console. This action does not delete the physical folder or any email messages it contains. To delete email messages use the Folders or Message History items in the Management section of the Management Console. To delete the folder on disk and its contents use Windows tools.

7.7.4.2 Configuring Default Folder Access

You can set the default folder permissions to control user ability to view and manipulate items in most MailMarshal folders.

To configure default access permissions for MailMarshal folders:

1. In the left pane of the Management Console, select **Policy Elements**. Then select **Folders** from the right pane menu. Click **Default Folder Security**.
2. This pane displays a list of security objects. Available object types include MailMarshal roles, MailMarshal Users, and Windows users and groups. Click an object name to show the permissions that role has over the features of MailMarshal folders.



Tip: Windows objects are only shown if Windows Authentication is used for the Management Console. To enable Windows Authentication, use the Config Service Admin Tool (see “Using the Config Service Admin Tool” on page 209).

Copyright © 2026 Trustwave Holdings, Inc.

- To add items to the list, click **Add** then select the items. You can see and add individual users by selecting an item and selecting **Show Users**. Each item you add is given full permissions by default.
- To delete an item from the list, select it and click **Delete**.

3. To change permissions for an item highlight the name. The lower pane shows the current permissions for this item. Set permissions by selecting the appropriate options.
   - A user could be a member of more than one role, and can also be listed individually. In this case, you can choose how permissions are applied by ordering the list. For details, see Help.
4. To save the changes, click **Save**.

7.7.4.3 Configuring Access for a Specific Folder

Set the permissions on a particular folder to control user ability to view and manipulate items in that folder. Permissions on a specific folder override the default folder permissions.

To configure access permissions for a specific MailMarshal folder:

1. In the left pane of the Management Console, select **Policy Elements**. Then select **Folders** from the right pane menu.
2. In the right pane, edit a specific folder. Enable the item **Override default folder security** to show the Security tab.
3. This pane displays a list of security objects as described above. Click a name to show the permissions that role has over the features of the specific MailMarshal folder.
   - To add items to the list, click **Add** then select the items. Each item you add is given full permissions by default.
   - To delete an item from the list, select it and click **Delete**.
4. To change permissions for an item highlight the name. The lower pane shows the current permissions for this item. Set permissions by selecting the appropriate options.
   - A user could be a member of more than one role, and can also be listed individually. In this case, you can choose how permissions are applied by ordering the list. For details, see Help.
5. To save the changes, click **Save**.
6. To apply the changes, click the **Commit** button in the toolbar.



Note: Setting access permissions for a folder in MailMarshal does not affect the Windows file permissions for the folder or items in it. To limit access through Windows, set the Windows access permissions for the MailMarshal Quarantine folder and all items in that folder on each MailMarshal email processing server.

To ensure that only the users with MailMarshal permissions can access these items, give full control of the Quarantine folder to the LocalSystem account or other account used by the MailMarshal services, and deny access to all other accounts.

Copyright © 2026 Trustwave Holdings, Inc.

7.8 Header Matching and Rewriting

MailMarshal 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 Content Analysis Policy rules.



Caution: 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.

7.8.1 Changing and Adding Headers with the Receiver

MailMarshal 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 Management Console, select **System Configuration** and then expand **Receiver Properties**.
2. Select **Header Rewrite** from the right pane menu.
3. You can add a new global header rewrite rule, edit an existing rule, or delete an existing rule. You can also change the order of evaluation of the rules. For details of the rule editing processes, see “Using the Header Rewrite Editor” on page 160.

7.8.2 Using Rules to Find Headers

You can search email headers using regular expressions using the MailMarshal Content Analysis Policy 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, add a new header match rule 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.

Copyright © 2026 Trustwave Holdings, Inc.

For details of the rule editing processes, see “Using the Header Rewrite Editor” on page 160.

7.8.3 Using Rules to Change Headers

You can alter email headers using regular expressions using the MailMarshal Content Analysis Policy 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 **Add.**

To perform more than one header rewriting action within a single condition, add a header match rule 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 Editor” on page 160.

7.8.4 Using the Header Rewrite Editor

This panel allows you to create a header matching or header rewriting rule. Header matching and rewriting uses regular expression matching and substitution. For more information about regular expressions, see “Regular Expressions” on page 221.

The header rewrite editor includes two tabs:

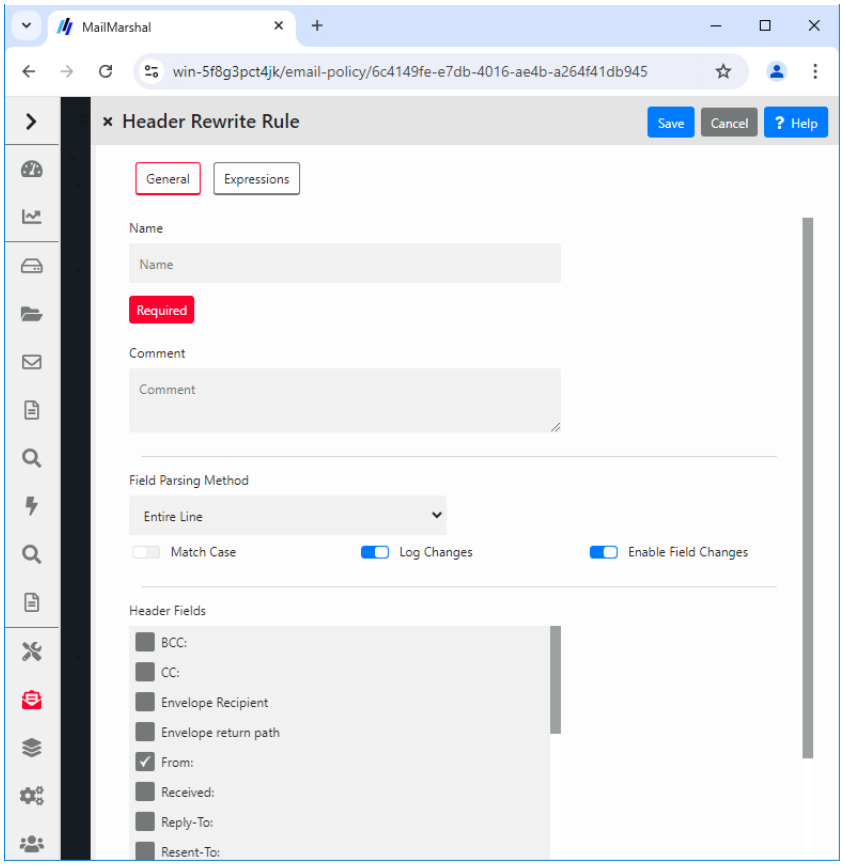
- On the General tab you can name the rule, select the header or envelope fields to be matched, select the portion of the field to be modified and choose logging options.
- On the Expressions tab you can enter matching and substitution expressions and test the rule.

You can also change the order of evaluation of header rewriting rules using the Move Up and Move Down buttons on the parent panel.

To use the Header Rewrite editor:

1. On the General tab, enter a name for the rewrite rule.
2. Optionally enter a comment to explain the purpose of the rule.

Copyright © 2026 Trustwave Holdings, Inc.



3. Choose a parsing method from the list. Depending on this selection, MailMarshal will apply regular expression matching to parts or all of the selected headers.

Note: To insert a custom header, use the parsing method “Entire Line.” To match or modify all email addresses, use the method “Email Address”.

- If you select the method “Entire Line” MailMarshal will use the entire text of the header as the input text for the substitution engine.
- If you select the method “Email Address” MailMarshal will use each email address found in the line as the input text.
- If you select the method “Domain” MailMarshal will use the domain part of each email address as the input text.

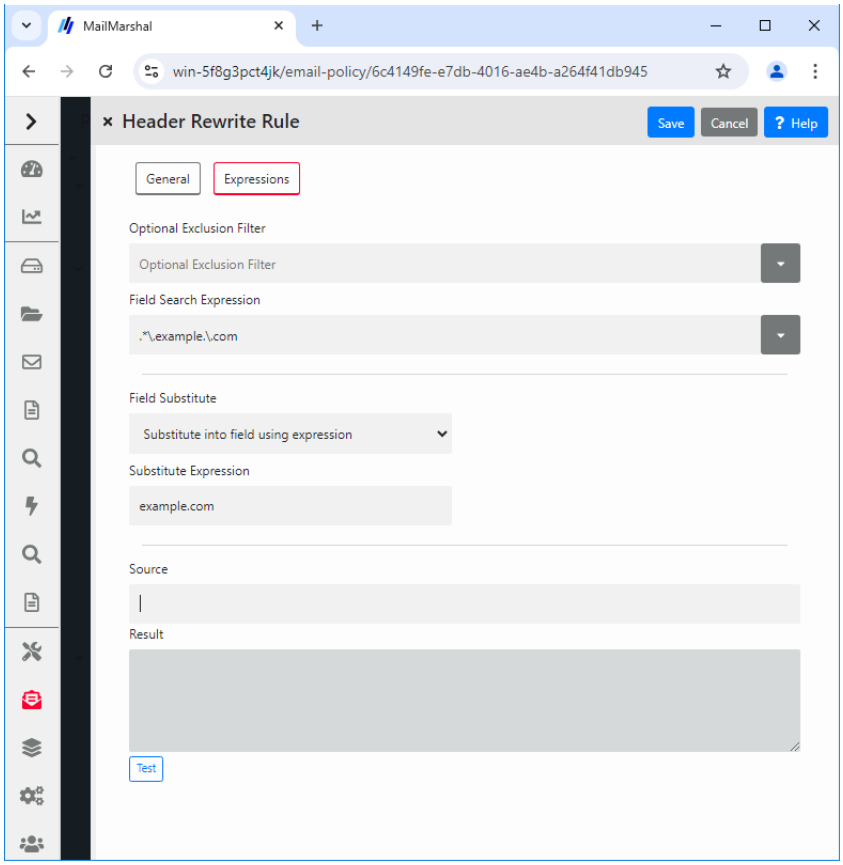
4. Select (toggle on) **Match Case** to perform a case sensitive search. Clear this option to make the search case insensitive.

Note: To search for email addresses or domains, use a case insensitive search.

5. *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 logs for the message. If only **Log changes** is selected, the logs will show the changes that would have occurred.

Copyright © 2026 Trustwave Holdings, Inc.

6. Select the fields that you want the rule to apply to from the list. You can add one or more custom header field names.
7. Click **Expressions** to continue.



8. In the **Optional Exclusion Filter** field, you can enter a regular expression. If this expression is found in the input text, the search will return “not matched”.
9. In the **Field Search Expression** field, enter a regular expression that MailMarshal should use to select the data for matching or rewriting. If the input text matches this expression, the rule will match or rewrite it, subject to exceptions based on the exclusion filter.
10. *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 details of syntax, see “Regular Expressions” on page 221. For details of where to place the file, see Help.

Copyright © 2026 Trustwave Holdings, Inc.

- **Delete the field** removes the matching material from the header. When **Entire line** is selected in the parsing options, selecting Delete the field removes the entire header line from the message.
- **Insert if missing** permits you to add a new header if any of the selected headers does not exist. MailMarshal 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.`



Note: In Content Analysis rule header rewriting, you can include MailMarshal variables in the Substitute or Insert text. For details, see Help.

11. To test the rule, enter an input string in the **Source** field and click **Test.** The result will appear in the **Result** field. For rewriting actions, the result will be the rewritten string. For matching, the result will be "matched" or "not matched".
12. *If this is a rewriting rule,* adjust the order of evaluation using the arrows provided below the list of rules.



Note: If you use several header matching rules within a single Content Analysis Policy 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 Content Analysis Policy rule action, the order of evaluation will be significant. Rewriting actions will be applied in top-down order as shown on the window.

7.9 Extending Functionality Using External Commands

An external command is a custom executable, Windows command, or batch file that can be run by MailMarshal. 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 Content Analysis Policy rule condition "Where the external command is triggered." For instance, you can invoke fgrep.exe for advanced expression matching.

If you want to use an external command to check for a condition, the command must return a standard return code.

You can also use custom executable files with the Content Analysis Policy rule action "Run the external command." For instance, a particular email subject line could trigger a batch file to start or stop a system service, or to send a page or network notification to an administrator.



Note: If a command action changes the message or attachments, you must set an option on the rule action to force the message to be repacked. For details, see "Run the external command" on page 115.

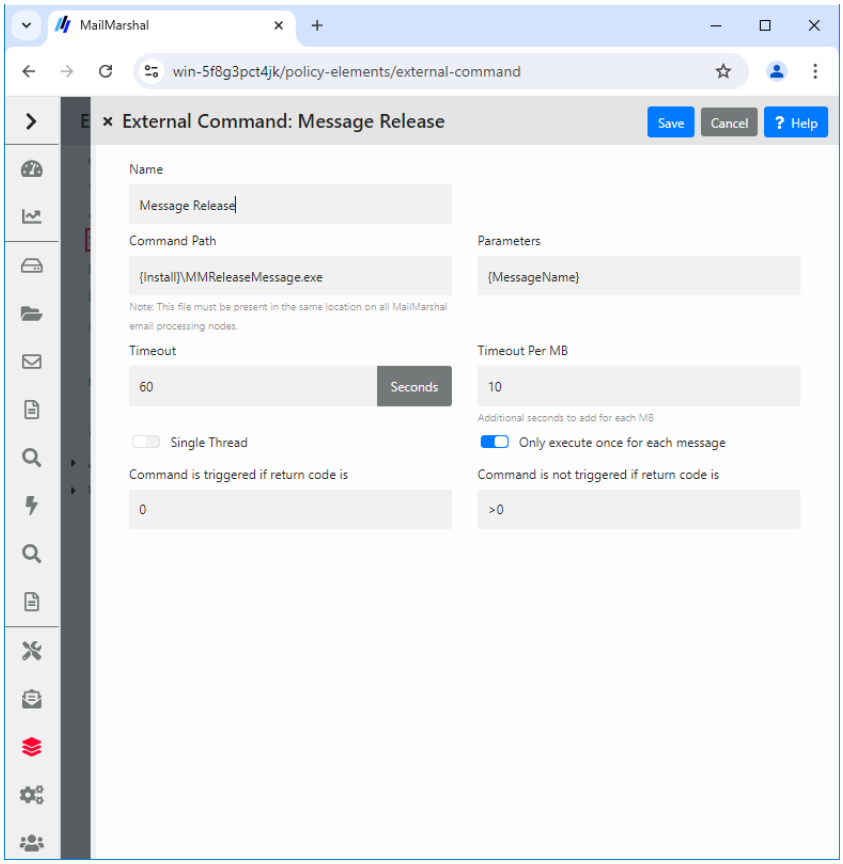
MailMarshal is provided with an external command for message release. See "Using the Message Release External Command" on page 215.

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

To create or edit an external command definition:

Copyright © 2026 Trustwave Holdings, Inc.

1. In the left pane of the Management Console select **Policy Elements**. In the right pane menu select **External Commands.**
2. To create a new external command, on the menu above the list click **Add.** To edit an existing external command, double-click an item in the list.



3. Enter a name for the external command.
4. Type the path for the executable file. You can also browse for the file by clicking **Browse**.

> **Note:** To use a batch file, you must invoke the command interpreter explicitly as follows:
> `%Systemroot%\system32\cmd.exe /C {batchfile.cmd} [variables...]`

5. In the **Parameters** field, enter any command line parameters necessary for the command. You can pass specific information about a message to the command using MailMarshal variables. Particularly note the variable `{CmdFileName}`.
6. 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.

7. The **Single Thread** setting indicates whether the command must operate on one message at a time, or can be invoked multiple times. In most cases this box should be left selected. You can multi-thread certain executable files.

Copyright © 2026 Trustwave Holdings, Inc.

8. The **Only execute once for each message** setting determines whether an external rule condition command will be run for each component of a message, or only once. For example if you are using fgrep to perform Regular Expression searches of attached files, this box should be cleared to ensure that MailMarshal passes each component of each message to fgrep.exe.
9. If you plan to use the external command as a rule condition, you must set the trigger return code information. You should find this information in the documentation of the executable.

Two fields allow you to enter trigger values which further specify the meaning of the code returned from the virus scanner.

- If the code returned matches any value entered in the field **Command is triggered if return code is**, MailMarshal 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).

7.10 Configuring Reputation Services

MailMarshal can retrieve information from DNS based blocklists or Reputation Services, including the Marshal IP Reputation Service and third-party services such as SpamCop and Spamhaus.

Configuring a DNS Blocklist for use in MailMarshal is a two step process. You configure details of the list in Policy Elements, then you configure one or more Connection Policy rules to filter email based on the list information

For more information about configuring Reputation Services, see “Controlling Who Can Send Email Through Your Server” on page 78. For details of the information on the Reputation Services window of the Management Console, see Help.

Copyright © 2026 Trustwave Holdings, Inc.

8 Monitoring Email Flow

MailMarshal provides a number of tools to assist in daily administration of email flow and server health. These include the Management Console, the Spam Quarantine Management Website, Marshal Reporting Console, Windows event logs, the Windows performance monitor, and the text logs generated by each MailMarshal service.

You can delegate access to a number of these tools, including the Console functions, reports, and spam management.

Table 23: Email monitoring options

If you want to:	Use:
View a summary of email traffic and filtering activity for the current day or other period	The Dashboard page in the Console. See “Monitoring Email Statistics and Server Health” on page 167.
View details of configuration update status and running MailMarshal services for each email processing server	The Status page in the Console. See “Monitoring Email Statistics and Server Health” on page 167.
View totals of messages processed and queued for each email processing server; delete a message queued for sending	The Mail Servers item in the Console. See “Deleting and Retrying Queued Messages” on page 168.
View a history of service alerts (unusual activity) for all MailMarshal servers	The Alert History in the Console. See “Viewing Alert History” on page 175.
Stop and start MailMarshal services	The Management item in the Management Console. See “Managing Node Services” on page 195.
View details of each message processed	The Email History, Folders, and Quarantine Audit in the Console. For more information, see “Viewing Email History” on page 173 and “Auditing Quarantine Actions” on page 175.
Search for details of a specific message	The History Search in the Console. For more information, see “Searching Folders and Email History” on page 174.
View, release, redirect, or delete a message in quarantine; report a message to LevelBlue as spam or not spam (if incorrectly classified)	The Email History, History Search, and Folders in the Console.
View a graphical display of performance information for the MailMarshal services	The Windows Performance monitor. For more information, see “Performance Monitor” on page 178.
View detailed debugging information for the MailMarshal filtering and delivery services	The Windows Application log and the MailMarshal text service logs on each server. For more information, see “Viewing Event History” on page 176 and “Using MailMarshal Text Logs” on page 178.
Generate detailed reports on email traffic and filtering activity over time	Marshal Reporting Console. For more information, see MRC documentation.

Copyright © 2026 Trustwave Holdings, Inc.

Table 23: Email monitoring options

If you want to:	Use:
Delegate administrative functions to help desk personnel	Management Console accounts and Folder Security options for each folder. For more information, see “Managing Authorized Users” on page 66 and “Working with Folders” on page 155.
Delegate management of spam and other quarantined messages to email users	The Spam Quarantine Management Website and the properties of folders. For more information, see “Setting Up Spam Quarantine Management Features” on page 210.

8.1 Using the MailMarshal Console for Email Management

The Console provides summary information on the current state of MailMarshal, as well as administrative access to the quarantine folders and message sending services.

8.1.1 Connecting to MailMarshal Using the Console

You can connect using a web browser from any computer that can browse to the Array Manager computer.

8.1.2 Monitoring Email Statistics and Server Health

The Dashboard and Status pages in the Console provide basic information about MailMarshal at a glance. To view these pages click **Dashboard** or **Status** in the left pane.

The Dashboard **Overview** includes:

- **Summary of email traffic:** Inbound and Outbound message totals and Blocked Threats total.
- **Email Security Score and Recommendations:** Analysis of the configuration of the MailMarshal installation, with best practice suggestions.
- **Blocked threat analysis:** Breakdown of threats by category.

The Dashboard **Emails** tab includes:

- **Hold Reasons:** Highlight of MailMarshal folders containing most blocked messages.
- **Rejected messages:** Detailed breakdown of reasons for rejections.
- **Rejected and held messages by user:** Highlight of users most affected by blocks.

The **Status** page includes:

- **Mail server health:** Service status, disk health, and alerts.
- **License status:** User count, license expiration, and maintenance expiration.
- **Automatic Updates status:** Last update and scheduled check times.

The Mail Servers page collects server and service status information for each MailMarshal email processing server. To view this item click **Mail Servers** in the left pane. For each server the Console

Copyright © 2026 Trustwave Holdings, Inc.

shows the server name, version of MailMarshal installed, whether the configuration is up to date with the configuration committed at the Array Manager, and whether the services are running.

For each server, you can also see details about the associated services and processed messages, as well as details of free disk space and event logs. To see a summary of the Receiver and Sender activity for a specific server, expand the **Servers** item then expand the item for the server name. To see details of the individual processing tasks, select an item (**Receiver, Sender,** or **Routes**). For more information see Help.

8.1.3 Deleting and Retrying Queued Messages

The **Sender** item for each server shows the messages MailMarshal is currently sending. The **Routes** item for each server shows a list of the route table entries that MailMarshal is attempting to send messages to, including items that are pending a retry and routes that are “down” or “on hold” (See “Marking Routes as Down” on page 187.)

You can stop sending a message that MailMarshal is currently sending and delete it. In the Sender view, highlight the message, and click **Kill Message.**

To attempt to send all messages queued for a specific route entry in the queue, in the Domains view, highlight a domain and click **Retry Route Now.**

The **Hold Queues** item for each server shows the number of items that are being held for each rule with a “Hold” action. To retry the rules, click **Retry Now**.

8.1.4 Viewing Folders and Folder Contents

MailMarshal message quarantine folders include the archive, parking and standard folders into which messages are placed through rule action, as well as the Dead Letter folders used for messages that cannot be processed, and the Mail Recycle Bin used to hold deleted items for a period.

To view a list of MailMarshal message quarantine folders, under Management expand the menu item **Folders.**

The Folders page shows a menu of folders. Visibility of folders in the list depends on the folder security permissions (see “Working with Folders” on page 155). To view the contents of a folder, select it in the menu. The contents display in the right pane, divided into daily sub folders. Select a daily folder to see its contents. By default no more than 250 items will be retrieved for each sub folder per screen. You can view the next or previous screen using the Page Up and Page Down keys. You can adjust the number of items per screen with the Rows menu at the bottom of the pane. You can select, order, and resize the columns in the list and save the column view, using controls on the page. You can sort the items on the screen by clicking column headers.



Note: The column sorting function only sorts the items on the current screen. If the folder contains more than one screen of items, sorting does not sort over multiple screens. Use the user filter at the top of the listing, or the search function, to retrieve a limited number of items.

You can also view items in the folders using the Email History view and the Search window.

Copyright © 2026 Trustwave Holdings, Inc.

8.1.5 Working With Email Messages

You can perform the following actions on an email message located in a MailMarshal quarantine folder:

View

Open a new window displaying the message headers, body, attachments, and the MailMarshal email processing logs if they are available for the message.

Forward

Send a copy of the message to a specified email address.

Delete

Move the message to the MailMarshal Mail Recycle Bin, or optionally delete it permanently. You cannot perform this action for items in Archive folders.

Release

Queue the message for action by other MailMarshal services. This action is typically used to deliver a quarantined message to the original recipient. You can choose from several options.

Spam

Forward a copy of the message to LevelBlue tagged as “spam.”

Not Spam

Forward a copy of the message to LevelBlue tagged as “not spam.”



Note: Use the Spam and Not Spam options to help improve MailMarshal spam detection by reporting messages that were wrongly classified. The messages you send are automatically processed. LevelBlue treats the messages in complete confidence.

To report a message you must have permission to forward messages from the folder that contains it. To configure permissions on a folder, see “Editing Folders” on page 157.

To work with a message, select it in the Email History, the Message Search results, or the Folders view.

8.1.5.1 Forwarding Messages

Use forwarding to send a copy of the message to a specified email address.

To forward a message:

1. Select the message.
2. Click the **Forward** icon on the toolbar, or open the message then choose **Forward** from the Message menu.
3. Enter one or more addresses. To forward to multiple addresses, enter them separated by semi-colons (for instance `RichardN@example.com; GeraldF@example.com`).

Copyright © 2026 Trustwave Holdings, Inc.

4. By default MailMarshal retains the message when you forward it from a quarantine folder. To adjust this behavior select or clear the check box. MailMarshal will not delete messages from archive folders.

8.1.5.2 Deleting Messages

Deleting a message sends it to the Mail Recycle Bin, or optionally deletes it permanently.

To delete one or more messages:

1. Select the messages. You can use shift and control click to multi-select.
2. Click the **Delete** icon above the list. The message(s) will be sent to the Mail Recycle Bin folder.
3. To permanently delete an item, delete it from the Mail Recycle Bin.

8.1.5.3 Restoring Messages

Restore from the Recycle Bin is not currently supported. This functionality will be provided in a future update.

Once MailMarshal places a message in a quarantine folder, it retains that message for the period configured in the properties of the folder, unless you choose to delete the message permanently.

The retention period applies even if the message is moved to the Mail Recycle Bin or restored. For instance, if the Spam folder has a retention period of one week, and MailMarshal moves a message to the Spam folder, then you delete it to the Mail Recycle Bin, it will be permanently deleted from the Mail Recycle Bin one week after it was first received.

8.1.5.4 Viewing Messages

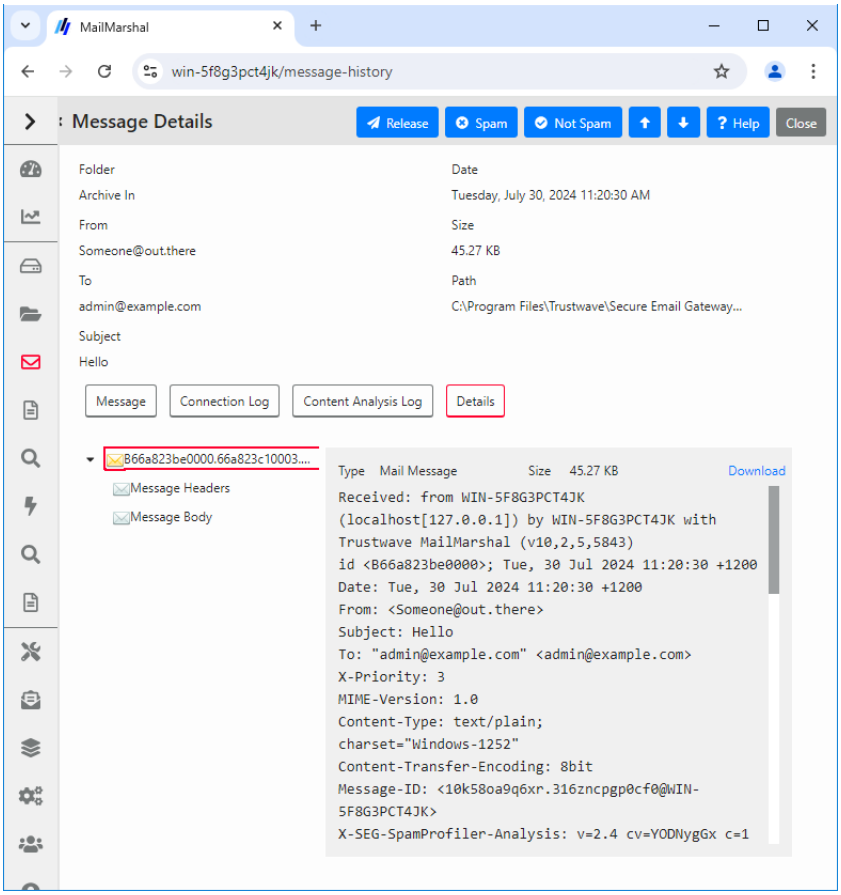
View a message to display the message headers, body, attachments, and the MailMarshal email processing logs if they are available.

To view a message and its associated processing logs in a folder, History, or Search view, double-click the message.

MailMarshal opens the message in a new panel.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 15: Message window



The lower portion of the message window includes several tabs: Message, Details, and one or more Log tabs. The Message and Details tabs restrict access to items that could represent security threats. Large images may be converted to thumbnails for performance reasons.

Message

Shows the message body in the richest available format (HTML, RTF, or plain text).

Details

Shows a tree view of the components of the message. You can click any item to view it in detail.

Log tabs

Show the MailMarshal processing logs for the message (Connection, Content Analysis, and Delivery logs)

The processing logs are available for all services that have processed a message (for instance, a quarantined message may not have a Delivery log). The logs are retained with the message, and may also be available for a longer period in the Sent History folder (depending on the retention period for that folder). You may also be able to retrieve this information from the main MailMar-

Copyright © 2026 Trustwave Holdings, Inc.

shal text logs. The text logs are created by default in the Logging sub folder of the MailMarshal installation folder. However by default these logs are only retained for five days.

You can copy message text to the Clipboard from any of the message tabs.

8.1.5.5 Releasing Messages

Releasing a message queues it for action by other MailMarshal services.

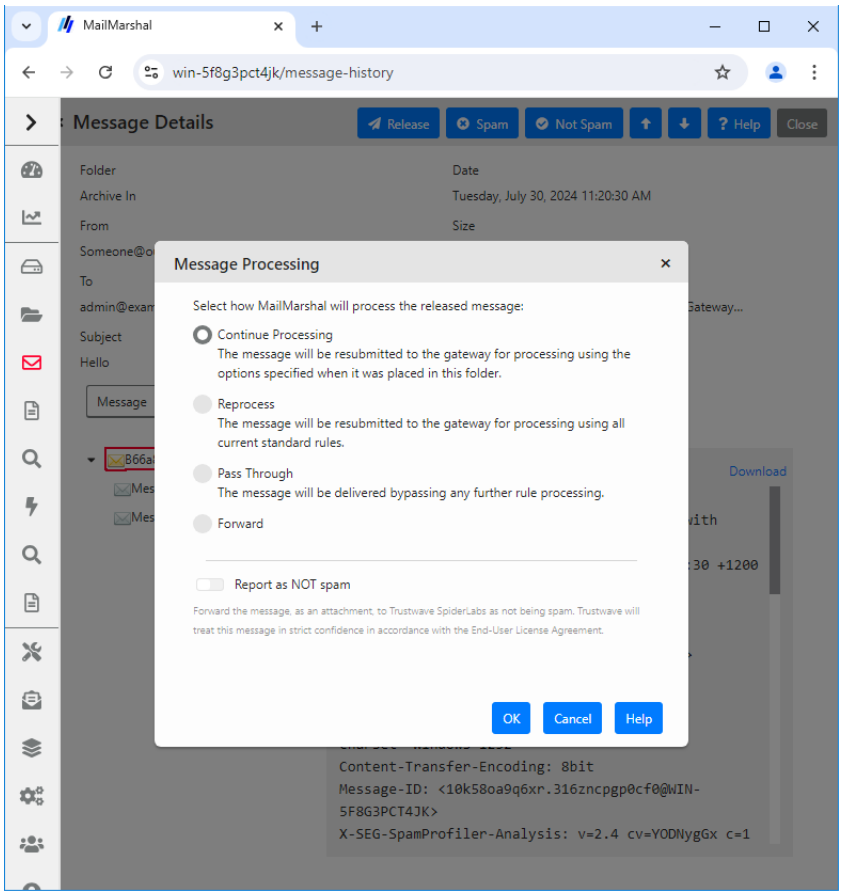
To release a message, select one or more messages, and then click **Release.**

Note: You can also release messages using a specially formatted email message. See “Using the Message Release External Command” on page 215.

You can add “fingerprints” of attached files into a list that MailMarshal can use in Rules. For more information, see Knowledgebase article Q10543.

The messages will be released for all recipients. By default the messages will be processed through additional rules, as specified for each message in the rule that placed the message in a folder.

Figure 16: Release Message window



To change the release actions, on the Release Message window, choose from the following actions:

Copyright © 2026 Trustwave Holdings, Inc.

Continue processing the message

This option continues processing the messages as specified for each message in the rule that placed the message in a folder. This is the default action. This action can be used to release a message from quarantine while testing it for any further violations of policy.

Note: If rules change after the message is placed in the folder, MailMarshal may not be able to perform the requested action. For more details, see Help for this window.

Reprocess the message

This option resubmits the message for processing by the current set of MailMarshal rules. This option can be useful to resubmit a number of messages after rules have been adjusted.

Pass through

This option queues the message for delivery with no further evaluation.

Forward

This option sends a copy of the message to an address you specify. After selecting this option, you can enter an email address.

The following additional options are available:

Report as not spam

Forward a copy of the message to LevelBlue tagged as “not spam.” To report a message you must have permission to forward messages from the folder that contains it. For more information about configuring permissions on a folder, see “Editing Folders” on page 157.

Keep a copy of the message

Once MailMarshal has completed the selected actions, by default it deletes the message from the folder (except archive folders). Check this box to retain the message in the folder

If the message has multiple recipients and you have chosen not to release it for all users, MailMarshal removes the users who received the message from the list of message recipients. In this case, if you select **Keep a copy,** MailMarshal keeps all existing users on the list. MailMarshal only deletes the message from a folder when it has no remaining recipients.

8.1.6 Viewing Email History

The Email History view shows each action taken on each message. Actions can include message classifications, moving to folders, delivery, and delivery failure among others. MailMarshal usually creates more than one history record for a specific message. If a history record records a move or copy to a folder and the message is present in the folder, you can use it to process the message exactly as you could from the folders view. Availability of items and actions in Email History depends on the security permissions for the folder where the item is found (see “Working with Folders” on page 155).

Copyright © 2026 Trustwave Holdings, Inc.

By default no more than 250 items will be retrieved per screen. You can view the next or previous screen using the Page Up and Page Down keys. You can adjust the number of items retrieved with the Rows menu at the bottom of the pane. You can select, order, and resize the columns in the list and save the column view, using controls on the page. You can sort the items on the screen by clicking column headers.



Note: The column sorting function only sorts the items that have been retrieved. If there is more than one screen of history, sorting does not sort over multiple screens. Use the user filter at the top of the listing, or the search function, to retrieve a limited number of items.

8.1.7 Searching Folders and Email History

You can limit the items displayed in the folders or email history using the Filter For field at the top of the listing.

Search the email history by choosing **Search** from the top right of the listing. You can choose from a large number of search criteria including dates, subject, classification, and email addresses. If you want to see only items that can be viewed and processed, search only for items in specific folders.

You can search using any combination of the following options:

Classification

Allows you to select a classification name, or “all classifications” to search all classifications. Classifications include both user classifications and system classifications such as “Delivered successfully”.

Folder

Allows you to select a folder name, or “all messages” to search in all folders.

Message Name

Allows you to enter a unique name MailMarshal has assigned to this message. MailMarshal includes this information in the headers of each message. You can enter the name alone (13 characters), or the name and edition (13.12 characters) to identify a specific edition of the message. You can add the server ID (13.12.4 characters). You cannot combine this option with any other option.

Date

Allows you to select the time and date when an action was logged. You can choose from pre-configured date ranges, or select **Custom** to define a range of dates. For instance, you can use this option to search for messages that were sent on a specific day.

What is the email address

Allows you to enter the address the message was sent to, from, or both. You can use wildcard characters. For more information about wildcard character syntax, see “Wildcard Characters” on page 220.

Copyright © 2026 Trustwave Holdings, Inc.

Subject

Allows you to find messages containing certain text in the subject line. You can use wildcard characters. For more information about wildcard character syntax, see “Wildcard Characters” on page 220. To search for messages with a blank subject, select (toggle on) **Search for blank subject.**

Size

Allows you to search for messages of a specific size or range of sizes. If you do not want to limit the search by size, select **Any Size** *(default value)*. With size ranges you can choose to search for messages inside the size range that you enter *(between)* or outside the size range *(not between)*

Search history items

Enable (toggle on) this option to return message history records including classifications, system actions, and messages that have been quarantined within the database retention time. Disable (toggle off) the option to return only messages currently in folders.

8.1.8 Searching Rejected Messages

The Rejected Messages view allows you to review attempted connections that were rejected due to server policy or Connection Rule action.

Search the email history by choosing **Search** from the top right of the listing. You can choose to search by dates, email addresses, and IP addresses of the attempted connection. See Help for details.

You can limit the items displayed in the results using the Filter For field at the top of the listing. You can navigate through multiple screens of results using the controls at the bottom of the list.

To see more details of a specific rejected message, double-click the item in the results.

8.1.9 Auditing Quarantine Actions

You can review actions taken on messages in quarantine, such as releasing or deleting a message.

To view and search quarantine audit records, select **Quarantine Audit** in the left pane of the Management Console. Quarantine Audit covers actions taken from the Management Console, SQM, Digests, and Message Release external command.

8.1.10 Viewing Alert History

MailMarshal generates alerts for specific events of interest. Some of the events included are services starting, stopping, or remaining idle for a longer than expected time.

To view a historical list of service alerts, select **Alert History** in the left pane of the Management Console.

Copyright © 2026 Trustwave Holdings, Inc.

8.1.11 Viewing Event History

Each component of MailMarshal writes messages to the Windows application log. Each event type is given a unique Event ID number. You can review these events using the Management Console or the Windows 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 review the event logs in the Management Console, select **Event History** in the left pane. When this node is selected, the right pane shows a filtered view of the Windows event logs for MailMarshal on the array manager and all email processing servers in the installation.



Note: You can view information about a specific email processing server by expanding its entry under **Mail Servers** and selecting the sub-item **Event History**.

MailMarshal provides several pre-configured filters you can use to limit the events being displayed.

You can also customize a filter, or search for a specific event.

You can click any event listed (standard view: double-click) to see the full details.

For more information, see Help.

8.1.12 Finding Events

The MailMarshal Event Log view allows you to filter the records you retrieve, or search for specific records.

8.1.12.1 Event Log Filter

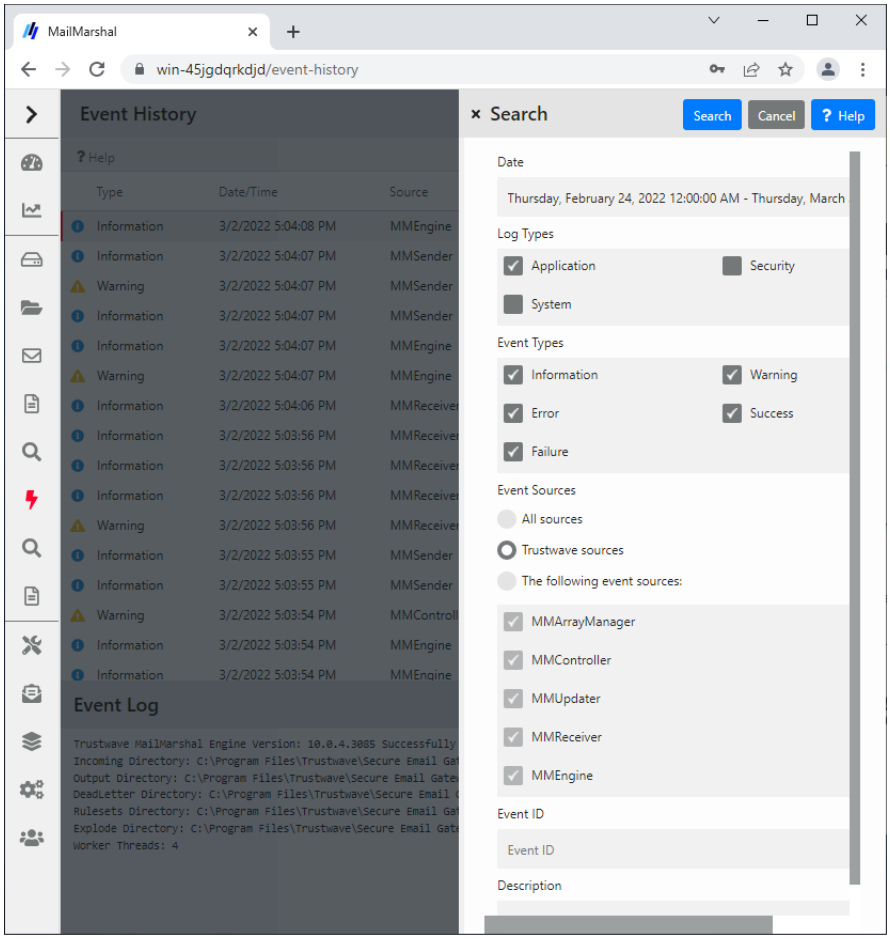
To filter the event history, enter text in the Filter For field at the top of the panel, and then click **Go**. To clear the filter, clear the field and then click **Go**.

8.1.12.2 Event Log Search

This panel allows you to search for specific events in the MailMarshal event log. To access the search panel, click **Search** at the top of the Event History panel.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 17: Event log search window



Enter parameters, then click **Search** to find matching items.

To return to the default view, reload the page.

For more information, see Help.

8.2 Using Windows Tools

MailMarshal provides information in a standard format through the Windows event log and performance monitor.

8.2.1 Event Log

Each component of MailMarshal writes messages to the Windows application log. Each event type is given a unique Event ID number. You can review these events using the Event Viewer. You can also use these events to trigger automatic actions such as pager notifications, service restarts, or popup notifications via third-party products. To open a custom view of the Event Log, use the Event History item in the Management Console.

Copyright © 2026 Trustwave Holdings, Inc.

8.2.2 Performance Monitor

Each core service of MailMarshal (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

8.3 Using MailMarshal Text Logs

Each MailMarshal service creates its own daily log files. These files provide a detailed record of routine processing and any problems encountered. The most recent information is at the end of the log file. The files are located in the Logging folder. By default, this folder is within the MailMarshal installation folder. MailMarshal keeps 6 days of log files by default.

Each message in the quarantine folders or Sent History includes the portion of the log file that relates to the message. You can see these message logs when you view a message in the Console. For more information, see “Working With Email Messages” on page 169.

Copyright © 2026 Trustwave Holdings, Inc.

9 Managing MailMarshal Configuration

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

9.1 Managing Your MailMarshal Licenses

MailMarshal requires a valid license key in order to process email. When you install MailMarshal, the installation process inserts a temporary license key valid for 30 days from the time of installation. Contact a LevelBlue Sales Representative to purchase the product and receive a full license key, or to request an extended trial. If you have received a valid full key, you can enter it at any time using the procedure given in “Entering a License Key” on page 180.

Install licenses at the array level. The licenses apply to all MailMarshal installations in an array.

Full MailMarshal license keys are normally keyed to the Windows domain SID. If you move the Array Manager server to a different domain the key will become invalid. MailMarshal will notify you and generate a temporary key valid for 14 days. You should immediately request a new key using the procedure given later in this section.



Note: MailMarshal is licensed according to the number of email users in your organization (excluding distribution lists and role accounts). The licensed number is encoded in the product key and shown in the Console. Exceeding the licensed number will not have any effect on email processing.

For computers not joined to a domain, LevelBlue can provide a key based on your computer SID or the list of local email domains.

9.1.1 Reviewing Installed Licenses and Maintenance

Use the Management Console to view the details of all installed license keys, including the key expiry date, maintenance expiry date, number of users, and any optional features licensed.

To view details of the currently installed license:

1. In the left pane of the Management Console, click **System Configuration.**
2. In the right pane menu, select **License**.

   This pane shows full information about the key and maintenance contract expiry. Information about maintenance expiry is retrieved daily from LevelBlue web servers. Current maintenance is required to use frequently updated features such as SpamCensor, SpamProfiler, and the Marshal IP Reputation Service.

   a. You can select how MailMarshal will behave if the license expires or becomes invalid.

      - If you select **Pass through all email,** MailMarshal will function as an email relay. MailMarshal will pass messages on to their destinations without applying any engine based policy
      - If you select **Halt all processing and hold all email**, MailMarshal will continue to accept messages so long as there is available disk space for the incoming queue. MailMarshal

Copyright © 2026 Trustwave Holdings, Inc.

will not deliver any messages until you enter a valid license or change this option to pass through all email.

b. To apply the selection, click **Save** and then commit the configuration.

9.1.2 Requesting a New License Key

To include all information required for LevelBlue to generate an appropriate key, request the key through the Management Console.

To request a new license key:

1. In the left pane of the Management Console, click **System Configuration.**
2. In the right pane menu, select **License**.
3. Click **Request Key.**
4. Complete the required information on the Request License Key panel. MailMarshal will append the information required to generate a unique key.



Tip: To assist in identifying your organization, include the Unique Customer Reference Number as found on order confirmations.

5. To email the request to LevelBlue, click **Send Request**.



Note: When you click Send Request, MailMarshal also places the additional request information on the Clipboard. You can paste this information to any application if you need to send a request manually.

9.1.3 Entering a License Key

When you receive a key from LevelBlue, use the Management Console to enter it and verify its validity.

To enter a license key:

1. In the left pane of the Management Console, click **System Configuration.**
2. In the right pane menu, select **License**.
3. Click **Enter Key.**
4. Enter the key, and select how MailMarshal will behave if the license expires or becomes invalid.
5. Click **Save.** MailMarshal will report the validity of the key you entered.
6. *If your key expired,* MailMarshal might have stopped the Engine service. Verify that all services are running on all email processing servers by completing the following steps:
   a. In the left pane of the Management Console, click **Mail Servers**.
   b. MailMarshal displays all servers in the array. Select a server and click **Server Properties**.
   c. *If a MailMarshal service is stopped,* click **Start**.

Repeat step c to verify each server service in your array is started.

Copyright © 2026 Trustwave Holdings, Inc.

9.2 Backing Up and Restoring the Configuration

You should back up your MailMarshal configuration at the following times:

- Before and after you make substantial MailMarshal configuration changes.
- Before applying an upgrade.

Note: You can make backups automatically once a day and/or after every configuration commit. Daily backups are enabled by default. See “Automatic Configuration Backup” on page 182.

You can restore the configuration when you want to make the following changes:

- Create a new Array Manager server.
- Return to a previous version of your email policy.

In addition to the following backup and restore procedures, you can back up and restore the configuration using a command line prompt. For more information see “Using the Configuration Export Tool” on page 207.

You can import your user and group information using the MailMarshal Management Console. For more information see, “Configuring User Groups” on page 127.

You can also import user group information using a command line prompt. For more information see “Using the Group File Import Tool” on page 205.

For more information about backing up the `\Quarantine` folders and the MailMarshal database, see the LevelBlue Knowledgebase.

9.2.1 Backing Up the Configuration

Backing up the MailMarshal configuration includes running Backup in the Management Console and backing up the following additional files:

Table 24: Files to include in configuration backup

Computer	Folder	Files
Array Manager	Folder you specify during Backup operation (by default, *InstallPath*\ConfigurationBackup)	manual or automatic backup zip file (for example, MailMarshal-*ver*-Manualbackup_*datetime*.zip)
Array Manager	*InstallPath*	filetype.cfg
Array Manager (*optional*)	InstallPath\Logging	*.log
Email processing servers	*InstallPath*\Quarantine and *InstallPath*\Quarantine\ValidFingerprints	*.*

Copyright © 2026 Trustwave Holdings, Inc.

Where `InstallPath` indicates the location where you installed the product. The default install path is `\Program Files\Trustwave\Secure Email Gateway`.



Note: Backups do not include members of groups imported through directory connectors.

To back up the MailMarshal configuration:

1. In the left pane of the Management Console, click **System Configuration.**
2. In the right pane menu, select **Backup**.
3. *If you use DKIM signing,* select the option to include DKIM keys.
4. Click **Backup Now**. The backup is created in the `ConfigurationBackup` subfolder on the Array Manager.



Tip: To ensure the backup is not deleted by the backup retention policy, copy this file to another location.

5. *If you have created file type rules*, back up the `filetype.cfg` file in the `\InstallPath` folder.
6. Make a note of each MailMarshal email processing server computer name.
7. On each MailMarshal email processing server computer, back up the `\InstallPath\Quarantine` and `\InstallPath\Quarantine\ValidFingerPrints` folders by following the instructions in Knowledgebase article Q10220.
8. Make a note of the MailMarshal database computer name.
9. On the database computer, back up the MailMarshal database by following the instructions in Knowledgebase article Q10221.

9.2.2 Automatic Configuration Backup

MailMarshal can back up configuration automatically. Automatic backup can be on a daily schedule and/or after each configuration commit. Daily backup is enabled by default.

Automatic backups include the same configuration items included in manual backups. To make a full automatic backup, you should schedule backup of the files mentioned in the previous section.

Automatic backups are stored in the subfolder `\ConfigurationBackup` within the MailMarshal installation on the Array Manager server. The backup file name shows the product version and date of creation.

To enable, disable, or set the retention period for automatic backups, in the Management Console navigate to **MailMarshal Properties > Array Properties > Backup.**

9.2.3 Restoring the Configuration

Restoring the MailMarshal configuration requires a number of steps. You can restore the configuration if you are creating a new Array Manager server, or if you want to return to a previous version of your email policy.

Copyright © 2026 Trustwave Holdings, Inc.

For additional steps required to restore a configuration saved in MailMarshal 8.2, see “Using the Configuration Export Tool” on page 207

Note: The restored data does not include the members of groups imported through directory connectors. **To retrieve the group members:** After restoring the configuration, in the left pane of the Configurator right-click User Groups and select **Reload User Groups**.

To restore your MailMarshal configuration:

1. In the left pane of the Management Console, click **System Configuration.**
2. In the right pane menu, select **Restore**.
3. Select a file to restore from the list. Backups are stored in the subfolder `\ConfigurationBackup` within the MailMarshal installation on the Array Manager server. The backup file name shows the product version and date of creation.
4. Click **Restore.** Enter the password to restore DKIM keys, and then click **OK.**
5. To restore custom file type definitions, copy the backup `filetype.cfg` file to the `\InstallPath` folder on the Array Manager computer.
6. To repopulate users in Azure Entra, LDAP and Active Directory user groups with current members:
   a. In the left pane of the Management Console, select Policy Elements. In the right pane, expand **User Groups**.
   b. For each Connector based group, select the group and then click **Reload**.
7. To retrieve the latest Spam Censor definition file, `spamfilter.xml`:
   a. From the left menu, select **System Configuration**.
   b. Select **Automatic Updates** in the **left pane** and click **Check for Updates Now.**
   c. When the update is complete, click **OK** and then click **Commit Configuration**.
8. On each MailMarshal email processing server computer, restore the `\InstallPath\Quarantine` and `\InstallPath\Quarantine\ValidFingerPrints` folders by following the instructions in Knowledgebase article Q10220.
9. On the database computer, restore the MailMarshal database from the backup copy. For more information about restoring a database file, see the Microsoft SQL Server or SQL Express documentation.
10. To connect to a new or existing MailMarshal database, connect to the database using the MailMarshal Server Tool. For more information, see “Joining a Node to an Array” on page 196 and “Working with Array Communications” on page 204.

9.3 Configuring Local Domains

You configure a list of local email domains when you install MailMarshal. You may need to update this configuration if you change internal email servers, or if you add more Internet domains.

Note: The list of local domains configured in MailMarshal should always match the DNS MX records that direct email from the Internet to MailMarshal.

Copyright © 2026 Trustwave Holdings, Inc.

You can specify delivery options for local domains as part of a Route Table. Delivery options include relay to an internal email server (known as a **relay domain** in earlier versions of MailMarshal), or POP3 delivery by MailMarshal (known as a **POP3 domain** in earlier versions of MailMarshal).

If you are using an array of MailMarshal email processing servers, you can choose to set different delivery routes on each email processing server.

Local Domain settings also include DKIM and DMARC configuration, and a list of details of "executives" used in fraud detection rules.

To view the list of configured Local Domains, in the left pane of the Management Console click System Configuration, and then select **Local Domains** from the right pane menu.

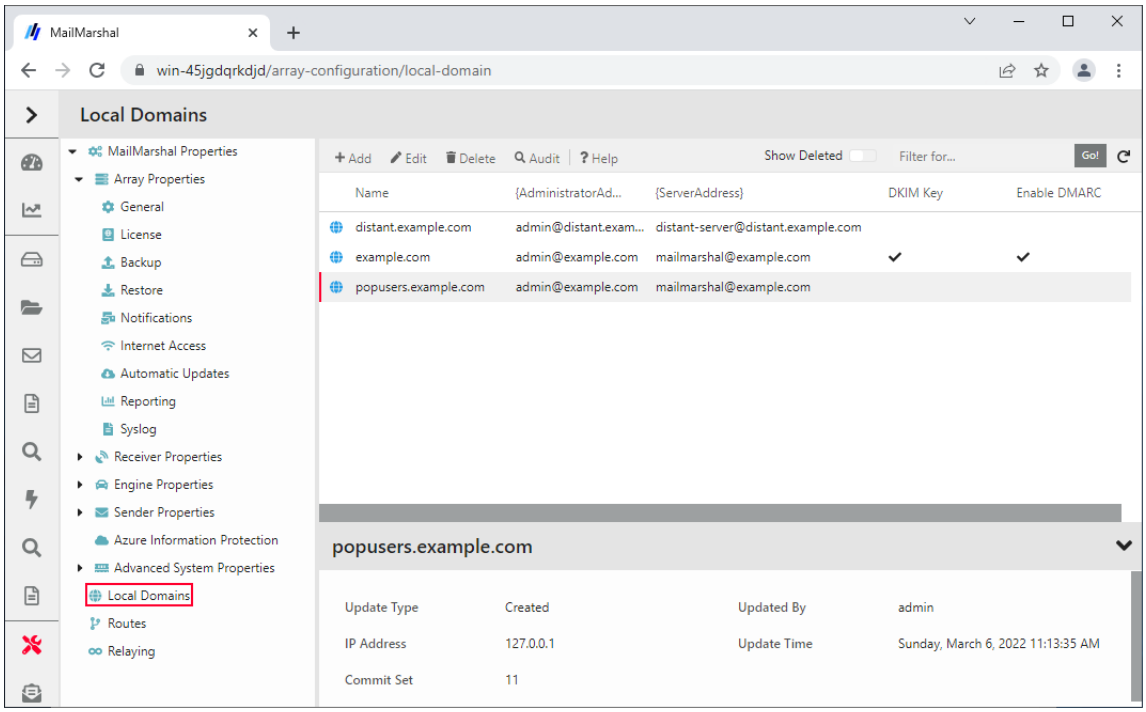
9.3.1 Changing Local Domains Information

You can change the list of domains MailMarshal recognizes as local.

Note: To change delivery locations for Local Domains, see "Configuring Routes" on page 185.

To change the list of local domains:

1. In the left pane of the Management Console click System Configuration, and then select **Local Domains** from the right pane menu.
2. The Local Domains window displays a list of the local domains, and the administrative addresses and other information associated with each domain.



3. Select the action you want to perform:
   - To create a new local domain listing, click **Add.**

Copyright © 2026 Trustwave Holdings, Inc.

- To edit an existing local domain listing, highlight it and then click **Edit.**
- To delete an existing local domain listing, highlight it and then click **Delete.**

For details of the fields on the Local Domain windows, see Help for each window.

9.4 Configuring Routes

MailMarshal uses Routing Tables to determine where and how to deliver email messages. When you install MailMarshal, the Configuration Wizard creates a basic Routing Table with a single entry for Local Domain email and a single entry for outgoing email.

You can add entries to the Routing Table to support a number of routing scenarios, such as:

- **Load Balancing:** Multiple entries for the same destinations, used alternately.
- **Fallback Delivery:** Additional entries for the same destination, used only when delivery fails.
- **Custom delivery** for a domain: Additional destination entries, used to deliver email addressed to specific local or remote domains through specific servers.
- **SMTP Authentication** for a route: Authenticated connection to the server that MailMarshal uses to deliver messages for the route.

A routing destination can be defined by an IP address, a host name, MailMarshal POP3, or DNS MX resolution.

You can create additional routing tables to support different routing from each processing server in a MailMarshal Array. For more information about advanced routing configuration, see Knowledgebase article Q11914.

To view the list of configured Routing Tables, in the left pane of the Management Console click System Configuration, and then click **Routes**.

9.4.1 Editing Routing Table Information

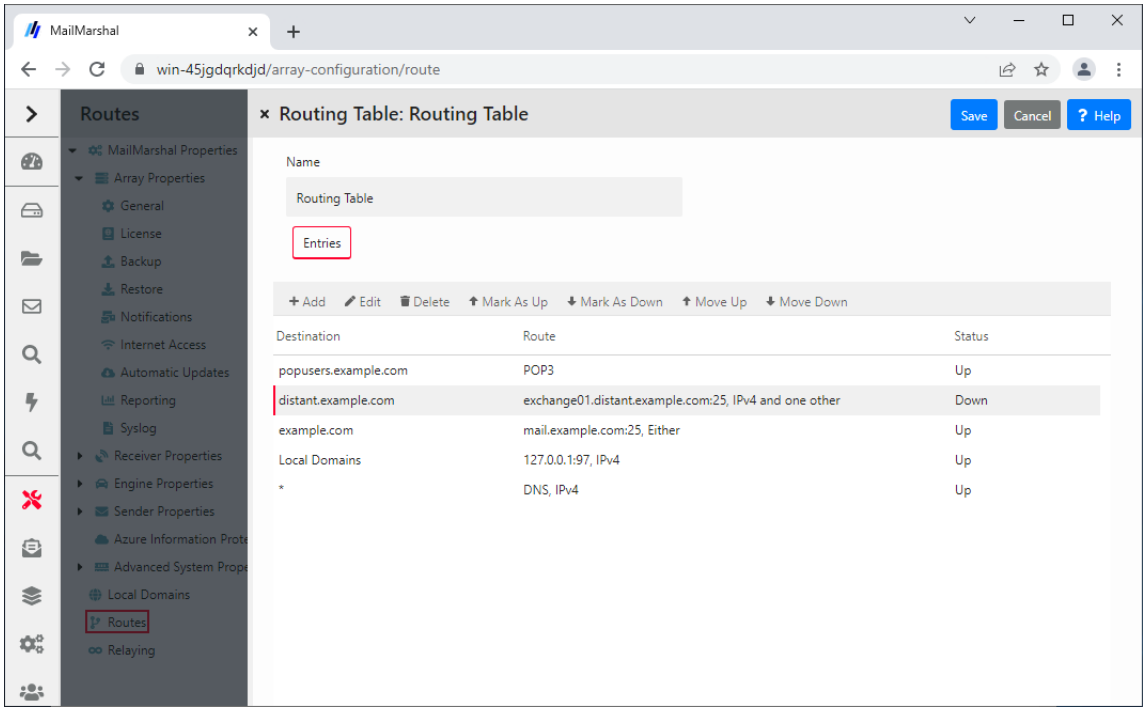
You can add new routing tables, and edit existing tables.

Note: To change the tables used for delivery, see “Configuring Delivery Options” on page 189.

To change the routing tables:

1. In the left pane of the Management Console click System Configuration, and then click **Routes**.
2. The Routes window displays a list of the routing tables.
3. *If you want to create a new routing table,* click **Add.**
4. *If you want to edit an existing routing table*, highlight it and then click **Edit.**

Copyright © 2026 Trustwave Holdings, Inc.



5. The Routing Table listing shows a list of destinations.

Note: A destination can be “Local Domains,” “Default Route” (normally used for delivery of outgoing messages and shown as *), or a specific domain.

Each destination entry can be associated with one or more routes.

Each route has a priority expressed as a number. Lower numbered routes to a destination will be used first.

For routes that are delivered by hostname or DNS, you can choose to use IPv4, IPv6, or either as available.

A route can support SMTP authentication (indicated in the table as [AUTH]).

Some routes can be marked as “down”. See “Marking Routes as Down” on page 187.

a. To create a new destination entry, click **Add.**

b. To associate a new route with a destination entry, on the Domain Routing window, click **Add.**

- If you want MailMarshal to deliver outbound email directly, set a destination of **Resolve using DNS** for the Default Route.
- If you want to send all outbound email to a firewall, or to a relay server at your ISP, add a route using the IPv4 address, IPv6 address, or host name. When you send outbound email to another server, that server is responsible for final delivery.
- If you want to create load-balanced delivery for a destination, add multiple routes with the same priority. (Set priority on the Advanced tab of the Route Entry window.)
- If you want to create a primary and fallback delivery option for a destination, set a lower number (higher priority) for the primary route. (Set priority on the Advanced tab of the Route Entry window.)

Copyright © 2026 Trustwave Holdings, Inc.

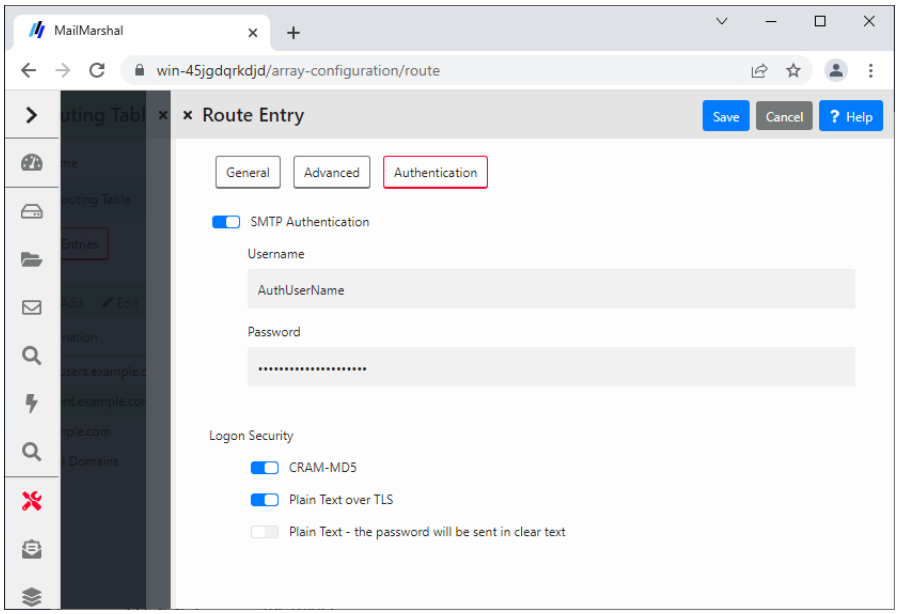
- To adjust the order of destination entries, use the arrow buttons on the route table window.

Note: If you have route table entries for specific domains, you may need to adjust the order of destinations to ensure proper handling. For example, consider the following routing table:

```
popusers.example.com      POP3
*.example.com             exchange01.example.com:25, IPv4
Local Domains             10.52.0.1:25, IPv4
* (default)               DNS, IPv4
```

In this order, email addressed to `popusers.example.com` is delivered to POP3 mailboxes on the MailMarshal server, but email addressed to any other subdomain in `example.com` is forwarded to the relay server `exchange01.distant.example.com` on `port 25`. If you change the sequence and put `*.example.com` first in the list, email addressed to `popusers.example.com` is relayed before it can be delivered to the POP3 mailboxes, because `pop.example.com` also matches `*.example.com`.

- If you want to use authenticated SMTP connections, select from the options on the Authentication tab of the Route Entry window. Determine the appropriate username, password, and supported methods from the administrator of the remote server. MailMarshal supports the CRAM-MD5, LOGIN, and PLAIN options for SMTP authentication. Additionally, authentication can be within a TLS session. For more information about the supported methods and behavior of this feature, see Help.



6. *If you want to delete an existing routing table,* highlight it and then click **Delete.**

For additional details of the routing table options, see Help for each panel.

9.4.2 Marking Routes as Down

For Routing Table destinations that are delivered to specific servers by FQDN, hostname, or IP address, you can suspend delivery by marking the route as “down”. This function can be useful if you

Copyright © 2026 Trustwave Holdings, Inc.

know that all servers for a particular domain will be out of service. When a route is marked as “down”, messages are queued, and the time a route is “down” does not count toward the message timeout. The status (Up or Down) displays on the Routing Table window. For more details of this functionality, see Help for this window.

9.5 Configuring Relaying

MailMarshal uses Relay Tables to determine which computers are allowed to send outgoing email through the MailMarshal installation. When you install MailMarshal, the Configuration Wizard creates a basic Relay Table that typically allows outgoing email from your Local Domain email server.

You can add entries to the Relay Table to support relaying from additional locations inside or outside your local network. Relaying is only allowed by explicit entries in the table.

Note: Some earlier versions of MailMarshal allowed relaying from the Local Domain server without requiring an explicit setting. This version requires an explicit entry in the Relay Table for each source.

You can create additional relay tables to support different relaying permissions from each processing server in a MailMarshal Array. For more information about advanced routing configuration, see Knowledgebase article Q11914.

To view the list of configured Relaying Tables, in the left pane of the Management Console click **System Configuration**, and then click **Relaying**.

9.5.1 Editing Relay Table Information

You can add new relay tables, and edit existing tables.

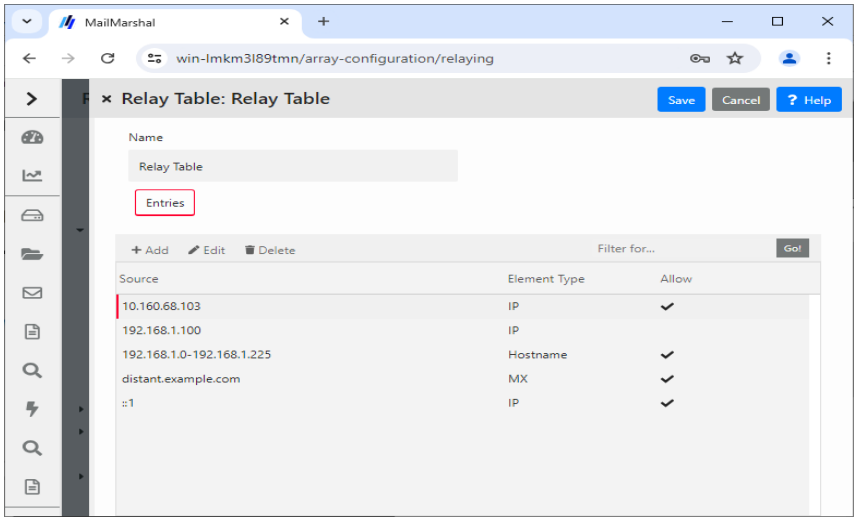
Note: To change the tables used to control relaying on each processing server, see “Configuring Delivery Options” on page 189.

To change the relay tables:

1. In the left pane of the Management Console click **System Configuration**, and then click **Relaying**.
2. The Relaying window displays a list of the relaying tables.
3. Select the action you want to perform:
   - To create a new relaying table, click **Add.**
   - To edit an existing relaying table, highlight it and then click **Edit.**
   - To delete an existing relaying table, highlight it and then click **Delete.**

   Each relay table can include multiple entries that define the servers allowed and denied relaying permission. You can use a single IPv4 or IPv6 address, a hostname, or a MX lookup for a domain.

Copyright © 2026 Trustwave Holdings, Inc.



For details of the relaying table options, see Help.

9.6 Configuring Delivery Options

MailMarshal distinguishes between “inbound” and “outbound” email.

Inbound email is email delivered to your organization. MailMarshal determines how to deliver this email based on your local domains. For more information about local domains see “Configuring Local Domains” on page 183.

Outbound email is email delivered to locations outside your local domains. MailMarshal can deliver this email directly using DNS lookups, or by forwarding all email to a relay host.

You configure basic delivery options using the Configuration Wizard when you install MailMarshal. You can make changes later if required.

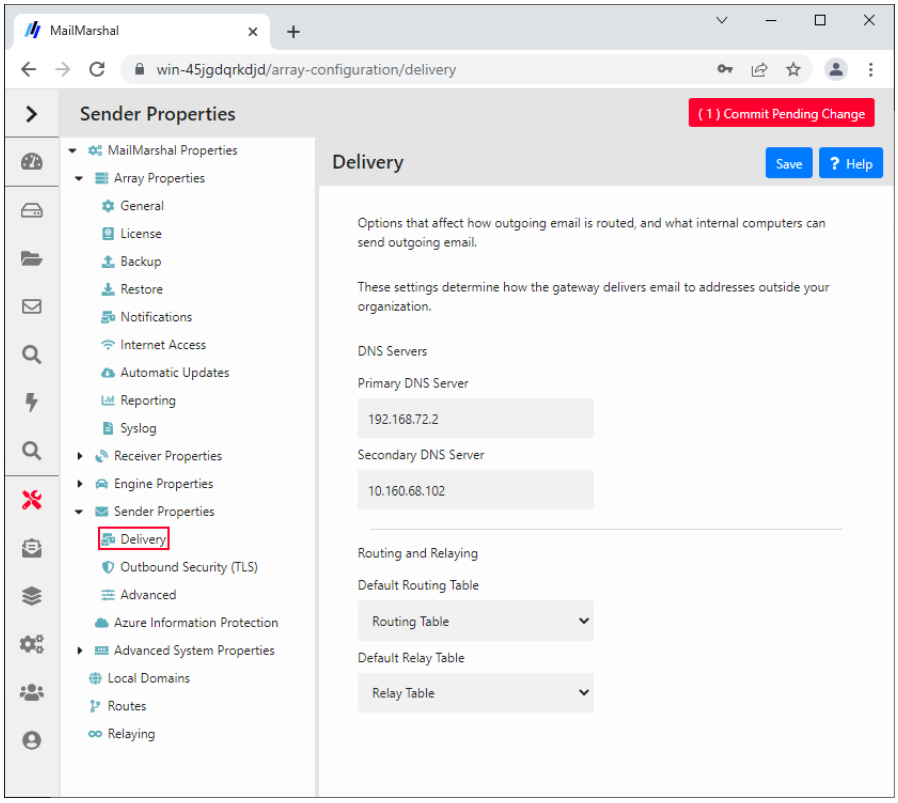
9.6.1 Configuring Default Delivery Options

You can make changes to default delivery options for the entire installation using MailMarshal Properties.

To configure delivery options:

1. In the left pane of the Management Console click **System Configuration**, expand **Sender Properties**, and then click **Delivery**.

Copyright © 2026 Trustwave Holdings, Inc.



2. Enter a primary DNS (Domain Name Server) address used by your organization. Optionally enter a secondary DNS address. These servers should be in the local network if possible, but in any case no further away than your ISP. They must be able to resolve domain names outside your organization.

Note: MailMarshal does not use the DNS servers configured in Windows networking.

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

3. Select a Routing Table that defines how MailMarshal should deliver email messages. For more information about Routing Tables, see “Configuring Routes” on page 185.
4. Select a Relaying Table that defines the servers MailMarshal will allow to send outgoing mail. For more information about Routing Tables, see “Configuring Relaying” on page 188.
5. To complete the changes, click **Save** on the MailMarshal Properties window and commit the configuration.

9.6.2 Configuring Delivery Options For A Specific Server

If you are using an array of MailMarshal servers, you can choose to set delivery options for each server.

To set delivery options for a specific server:

1. In the left pane of the Management Console click **Mail Servers.**
2. Select a server in the list and click **Edit**.

Copyright © 2026 Trustwave Holdings, Inc.

3. Click the **Delivery** tab.
4. Select **Customize the Delivery Settings.**
5. Change the entries as desired. For details of the fields and settings, see “Configuring Default Delivery Options” on page 189.

9.7 Setting Up Accounts

MailMarshal accounts consist of a user name and password. You can use accounts for two purposes:

- To authenticate user connections using a Connection Policy rule, or check for authenticated connections using a Content Analysis rule. For more information, see “Where sender did/did not authenticate successfully” on page 111 and “Where the DKIM verification result is” on page 109.

  Note: If you use this feature to allow one or more accounts to relay email, consider the following best practices:

  Ensure that these accounts have strong passwords. If an account password is guessed by a malicious person, MailMarshal could become an open relay. Change the passwords periodically.

  Use accounts that are only used for this purpose, and not Windows accounts with other permissions. Password transmission during authentication is not strongly secured.

  You can also check authentication using an Active Directory group. This option does not require you to enter account details in MailMarshal. It may be useful if many accounts are allowed to authenticate, or if accounts change frequently. For details, see Knowledgebase article Q16649.

- To specify users for the MailMarshal POP3 server. If you will be using accounts for POP3 delivery, set up a default routing table with POP3 routing for all required domains before creating accounts. For more information about POP3 domains, see “Editing Routing Table Information” on page 185.

  Note: The MailMarshal POP3 server is not designed to be used in an installation with more than one email processing server.

9.7.1 Creating Accounts

Create accounts using the MailMarshal Management Console.

To create accounts:

1. In the left pane of the Management Console click **Policy Elements**, and then click **Accounts**.
2. Click **Add**.
3. Enter the details for the user name and authentication information in the New Account window.
4. Enter one or more appropriate SMTP aliases for email delivery to this account's POP3 mailbox. Enter the complete addresses. Use the Enter key to complete each entry. Only use domain names

Copyright © 2026 Trustwave Holdings, Inc.

for which MailMarshal is functioning as a POP3 local domain server, based on the active Routing Table.



Note: If the routing table includes POP3 delivery for "Local Domains," you can enter the special value `Local Domains` for the domain part of the alias (for example, `someuser@Local Domains`). This entry ensures that email directed to the account name at any local domain will be correctly delivered. This value is case sensitive and the space between words is required.

If you want to use the account only for authentication, type `none`.

If you enter the same SMTP alias in more than one POP3 account, messages directed to that alias will be delivered to all of the mailboxes.

5. If the password fields are blank, MailMarshal will use Windows authentication to determine access for this account. In this case, ensure that the account name matches the name of a valid Windows user account that can be authenticated on all email processing servers.
6. To add the account, click **Save.**
7. Continue to add other accounts.
8. Click **Commit Configuration Changes**.

9.7.2 Editing Existing Accounts

Edit an account to change the password or email addresses associated with the account.

To edit an existing account:

1. In the left pane of the Management Console click **Policy Elements**, and then click **Accounts**.
2. Double-click the account you want to edit.
3. Change the password and aliases as required.
4. Click **Save.**

9.7.3 Deleting Accounts

Delete accounts that are no longer required. If you delete an account used for email delivery, you should also delete the delivery folder from the MailMarshal sending queue directory.

To delete an account:

1. In the left pane of the Management Console click **Policy Elements**, and then click **Accounts**.
2. Select the account you want to delete.
3. Click **Delete**.
4. To remove the delivery folder, on the processing server use Windows Explorer. Within the MailMarshal installation navigate to the `\Queues\Sending\` directory.
5. Back up the contents of the subdirectory for the account that you deleted.
6. Delete the subdirectory.

9.8 Configuring Email Batching

MailMarshal supports batch receipt and sending of email messages where you do not want to have an on-demand connection to the downstream email server. Mail batching is implemented through the

Copyright © 2026 Trustwave Holdings, Inc.

`MMGetMail.exe` helper application. You can use this application in batch files or custom scripting. For more information about `MMGetMail`, see Knowledgebase article Q10285.

Note: The integrated Mail Batching and Dial-Up Networking functions that were available in earlier versions of MailMarshal have been discontinued.

9.9 Configuring DKIM

MailMarshal can sign and validate messages with DomainKeys Identified Mail (DKIM). Signing can be controlled by policy, and validation results can be used in policy conditions.

To use DKIM for received messages you must enable message validation. To use DKIM for sending from local domains, you must enter key information for each local domain and then add a rule to apply signatures.

To configure DKIM validation:

1. In the left pane of the Management Console click **System Configuration**.
2. From the right pane menu expand Receiver Properties and select **DKIM**.
3. To enable DKIM validation, check the box **Enable DKIM Detection.** To disable the feature, clear the box.
4. To apply the changes, commit the configuration.

To configure DKIM keys for local domains:

1. In the left pane of the Management Console click **System Configuration**.
2. In the right pane, click **Local Domains**. Select a domain, and then click **Edit**.
3. Click the DKIM tab.
4. Click **Add** to generate or import a key, and select appropriate settings. For details, see Help.

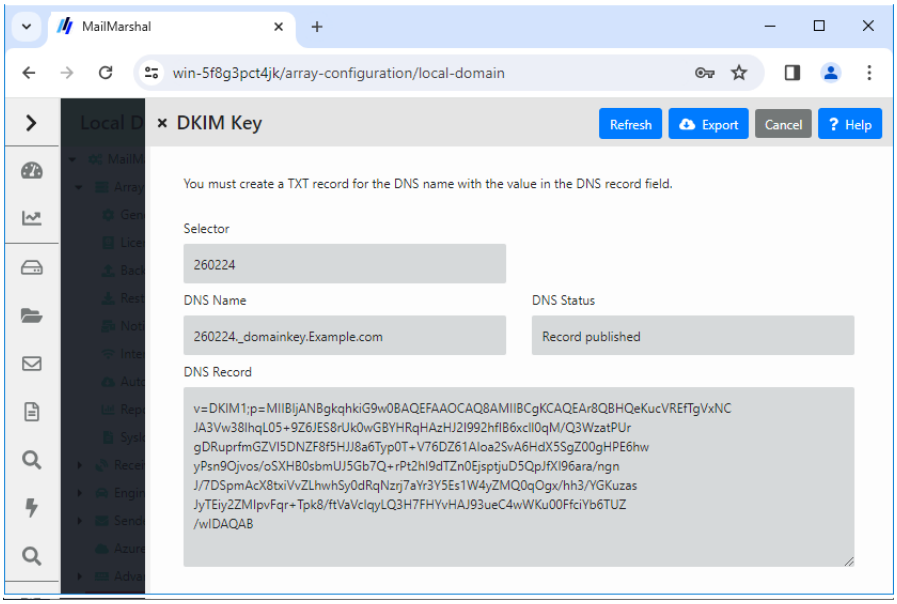
Note: Keep a copy of the key file in a secure location. DKIM signing keys are not included in the MailMarshal configuration backup.

5. Ensure that you have published a DNS TXT record that includes the related public key. The DKIM Key window provides the appropriate record text for the key.

Note: The TXT record will have a name like *`selectorname`*`._domainkey.`*`domain.TLD`* (for example, `20190822._domainkey.example.com`).

For more information about creating and publishing keys for DKIM, see Knowledgebase article Q20841.

Copyright © 2026 Trustwave Holdings, Inc.



6. **To sign messages**, once the DKIM key is created and published, use a Content Analysis Rule to apply the DKIM signature. See “Apply DKIM signature” on page 118.

9.10 Configuring DMARC

MailMarshal can participate in DMARC for local domains you specify. DMARC relies on SPF and DKIM. For an overview of all required configuration, see LevelBlue Knowledgebase article Q20650.

To use DMARC, you must set up information for one or more local domains and then enable DMARC for each domain. You can then choose to configure Content Analysis rules to take action on incoming messages depending on the results of DMARC validation.

Important: Enabling DMARC for a local domain causes DMARC validation and reporting to be performed for all messages addressed to the domain, as well as including the required DMARC information with each message sent from the domain through MailMarshal. This behavior is required by the DMARC framework.

To configure DMARC for a local domain:

1. In the left pane of the Management Console click **System Configuration**.
2. In the right pane, click **Local Domains**. Select a domain, and then click **Edit**.
3. Click the DMARC tab.
4. Ensure that a DMARC DNS record has been found and displayed. If a record does not display, investigate further that the record does exist and will be propagated to public DNS.
5. Select **Enable DMARC**.
6. Configure and enable rules to apply DMARC policy and accept DMARC reports. Rules are included in the default rules for new installations, and in a special policy group that is created on upgrade.

You can review DMARC results by sending DMARC report email to a third party site.

Copyright © 2026 Trustwave Holdings, Inc.

9.11 Managing Array Nodes

A MailMarshal installation consists of an Array Manager and one or more email processing servers, also known as array nodes.

9.11.1 Managing Node Services

You can view the status of the MailMarshal services on each email processing node, and stop or restart the services, from the MailMarshal Management Console.

To see an overview of the status of services on each node, in the left pane of the Management Console click **Mail Servers.**

To see details of the status of services on a particular node, and to stop or restart the services:

1. In the left pane of the Management Console click **Mail Servers.** The list shows all servers and a summary of the state of each server. (For more details about the information listed, see Help.)
2. In the right pane select the server you want and click **Edit**.
3. Select **General** from the left pane to see the Services listing and to see the status of each service installed on the node.
4. To stop one or more services, select them in the list then click **Stop.**
5. To start one or more services, select them in the list then click **Start.**
6. To restart all services, click **Restart all**.



Note: If you stop services from this window, they will remain stopped until you start them. Committing the configuration will not start the services.

9.11.2 Adding and Deleting Nodes

You can add email processing servers (nodes) to a running MailMarshal installation to add capacity or redundancy. You can also delete existing nodes from an installation.

9.11.2.1 Adding a Node

You can add a node at any time without affecting other nodes. After adding the node, adjust email routing so that the new node shares in email processing. Contact your Internet Service Provider or DNS administrator, as necessary.



Note: Adding a node does not create automatic load balancing.

To add a node to a MailMarshal installation:

1. Log on to the new server.
2. Install MailMarshal.
3. During installation, select the option “I want to join an existing array” and enter the name of the existing Array Manager.

Copyright © 2026 Trustwave Holdings, Inc.

- You must provide both a Windows account that can connect to the Array Manager, and an Array Join credential managed through the MailMarshal Server Tool.

For more information, see “Installing MailMarshal as an Array” on page 42.

9.11.2.2 Deleting a Node

You should delete a node to cleanly remove it from the MailMarshal array. Before deleting a node, adjust email routing so that the node to be deleted does not process any email. Contact your Internet Service Provider or DNS administrator, as necessary.

To delete a node from a MailMarshal installation:

1. Stop MailMarshal services on the node using the MailMarshal Management Console.
2. If you want to preserve messages from quarantine folders stored on the node, back up the Quarantine folder in the MailMarshal installation folder on the node.
3. Uninstall MailMarshal on the node server using the Add/Remove Programs application in Control Panel.
4. During the un-installation process, MailMarshal will attempt to remove the node records from the array installation.
   - To remove the node records from configuration you must provide both a Windows account that can connect to the Array Manager, and an Array Join credential managed through the MailMarshal Server Tool. Currently this is the only way to remove a node from configuration.
5. In the Management Console, an un-installed node that has not been removed will show a blank status.

9.11.3 Joining a Node to an Array

You can join an email processing server (node) to a MailMarshal array. After joining the array, the node will retrieve policy configuration from the Array Manager.

To join an existing node to a MailMarshal installation:

1. Log on to the node server.
2. Run the MailMarshal Server Tool from the MailMarshal program group.
3. On the Node > Array page, enter the local port, and the port and server name for the Array Manager. Select **Join Array,** and then click **Apply.**
   - You must provide both a Windows account that can connect to the Array Manager, and an Array Join credential managed through the MailMarshal Server Tool.

9.11.4 Customizing Settings for Nodes

Since the purpose of a MailMarshal array is to replicate configuration over a number of processing servers, most settings will be the same for all nodes. You can configure the following settings for each node:

Copyright © 2026 Trustwave Holdings, Inc.

Server name and general information

For each email processing server, you can view and change the server name and the description and location notes.

Note: Only change the server name here if you have changed the computer name of the email processing server.

Delivery information

For each email server in an array, you can specify DNS servers, and the relay and routing tables to use. One use of this override would be to allow geographically separated MailMarshal servers to deliver inbound email to different internal email servers.

Internet Access information

For each email server in an array, you can specify proxy settings (or direct access) that will allow the server to retrieve SpamProfiler updates over the Internet.

Inbound TLS information

For each email server in an array, you can configure Transport Layer Security (TLS) usage including a certificate.

Server Threads

For each email server in an array, you can configure the number of processing threads used.

Advanced server information

For each email server in an array, you can choose one or more IP addresses and ports the MailMarshal Receiver will bind to. You can specify what percentage of available threads each address:port can use. This setting allows you to reserve some Receiver capacity for specific connections (for instance to ensure that outgoing email will be accepted even if incoming volume is high)

Note: By default, the Receiver binds to port 25 on all configured IP addresses. This setting allows MailMarshal to receive all email sent to each email processing server at the default SMTP location. If you customize the Receiver bindings, ensure that you add a setting for each configured address.

You can specify a host name, which may be required if this information is not entered in the Windows networking properties. You can also select whether the email processing server should be preferred by the Array Manager as a host to be used in sending notifications.

9.12 Understanding Secure Email Communications

MailMarshal allows you to secure outgoing and incoming email using transport layer security (TLS), an implementation of secure sockets layer (SSL). MailMarshal supports the enhanced security of Perfect Forward Secrecy (PFS).

Copyright © 2026 Trustwave Holdings, Inc.

TLS secures the privacy of the communications channel and provides one-way authentication. TLS is generally used to provide a secure (encrypted) transport over which email communications including the headers, body and attachments are delivered. TLS can also assist in verifying server authenticity.

Use TLS when you want to secure your organization's email from being read by unauthorized users inside or outside of your organization. Secure email may be required if your organization sends or receives mail containing information that is protected under laws, such as the US Health Insurance Portability and Accountability Act (HIPAA).

TLS uses public-private key pair encryption on each MailMarshal server to secure an email communications channel and to authenticate itself to clients.



Note: TLS slows your email operations to a limited degree.

TLS works only when ESMTP (EHLO extensions) is enabled. (This is the default setting.) TLS does not work with HELO.

9.13 Securing Email Communications

You can use MailMarshal to secure incoming and outgoing email communications. MailMarshal allows you to decide where and under what conditions you want to use TLS. Setting up TLS involves three tasks:

1. Creating or importing a TLS Certificate
2. Enabling TLS for mail incoming to MailMarshal
3. Enabling TLS for mail outbound from MailMarshal.



Note: For more information about configuring TLS, see Knowledgebase article Q11636.

When TLS is configured, you can use rules to take action on incoming messages based on the use of TLS and details of the SSL certificate used by the remote server.

9.13.1 Working with Certificates

Each MailMarshal server using TLS makes its secure status public using a certificate. MailMarshal stores TLS Certificates on each server. For each MailMarshal server with which you want to use TLS, you must generate or obtain an authentication certificate. To perform these tasks, use the TLS Certificate Wizard.

Certificates have expiration dates. Starting two weeks before a certificate expires, MailMarshal sends a daily renewal reminder email to the MailMarshal administrator.

The TLS Certificate Wizard allows you to perform the following tasks:

- Generate a Certificate Signing Request (CSR) that you submit to a third-party certificate authority
- Import X.509 and PKCS#7 key-certificate backup files supplied by a certificate authority
- Generate self-signed certificates

Copyright © 2026 Trustwave Holdings, Inc.

- Save server-specific key-certificate pairs as PKCS#12 files
- Import PKCS#12 files

To create or manage certificates:

1. In the left pane of the Management Console, expand **Mail Servers.**
2. In the right pane listing of servers, edit the MailMarshal server for which you want to configure TLS.
3. Click **Inbound Security (TLS)**.
4. Click **TLS Certificate Wizard**.
5. Enter the required information on each tab to complete the certificate task you are performing. For more information about the workflow and the fields on each tab, click **Help**.
6. On the server pane, click **Save**.

9.13.2 Securing Inbound Communications

Using TLS is optional for incoming email. You can enable or disable TLS, and set the minimum required cipher strength for inbound connections. You can enable Perfect Forward Secrecy (PFS) by selecting an Elliptic Curve to be used for key exchange.

MailMarshal requires you to set incoming email TLS configuration on each email processing server in an array. Repeat the following task for each email processing server.

To enable TLS for inbound connections on a MailMarshal email processing server:

1. In the left pane of the Management Console, expand **Mail Servers.**
2. In the right pane, select **Servers** and then select the name of the email processing server for which you want to configure TLS.
3. Click **Inbound Security (TLS)**.
4. Specify the appropriate values. For more information about the options, click **Help**.



Note: The **Enable TLS** option is available only when a valid certificate is installed on the server.

5. On the server pane, click **Save**.
6. Commit configuration changes.

When a message is received with TLS, the Received: header line is marked with the version of TLS and the cipher used. For instance:

```
Received: from client03 (Not Verified[127.0.0.1]) by vm-example03 with
Trustwave SEG (v10,0,662,1) (using TLS: TLSv1, AES128-SHA).
```

You can use Connection or Content Analysis rules to take action based on the TLS status, the TLS protocol that was used, and the SSL certificate that was used. You can choose to classify, accept, reject, or quarantine messages depending on the information encoded in the certificate. You can check the validity date, permitted certificate use, certificate domain, trust, and revocation status. For

Copyright © 2026 Trustwave Holdings, Inc.

full details of the available options, see Help for the Rule Condition “Where the TLS client certificate matches criteria.”



Note: Ensure that the processing servers can connect to Internet locations using HTTP and HTTPS. This access is required for checking of Certificate Revocation Lists. You can use a proxy server for web access if required; see “Customizing Settings for Nodes” on page 196.

9.13.3 Securing Outbound Communications

Using TLS is optional for outgoing email. You can enable TLS, require TLS for specific domains, set the minimum cipher strength, and choose whether to offer a client certificate when requested by a remote server. Outbound TLS uses Perfect Forward Secrecy (PFS) if advertised by the remote server.

MailMarshal applies the TLS configuration for outbound email across all email processing servers in the array.

To enable TLS for outbound email:

1. In the left pane of the Management Console, click **System Configuration.**
2. In the right pane, expand **Sender Properties > Outbound Security (TLS)**.
3. Specify the appropriate values. For more information about the options, click **Help**.
4. On the server pane, click **Save**.
5. Commit configuration changes.

When a message is sent using TLS, MailMarshal classifies the message as “Delivered successfully over TLS.” You can review this information in the Console, and report on it using Marshal Reporting Console.



Note: You can also require delivery over TLS based on rule conditions. See the rule action “Deliver the mail via TLS only” on page 117.

9.14 Setting Advanced Options

MailMarshal allows you to configure a number of advanced settings. These settings default to values that are reasonable in the majority of cases. In specific cases you may need to change them. For full details of the settings, see Help for each pane on the Advanced Setting window.

9.14.1 MailMarshal Properties – Advanced

These options affect delivery and processing of email. If more than one MailMarshal server is included in an array, these options affect all servers. Some options can be overridden for each processing node (see “Customizing Settings for Nodes” on page 196).

Engine Blended Threats exclusions

Allows you to maintain a list of domains (or domain wildcard patterns) that will never be rewritten for Blended Threat scanning.

Copyright © 2026 Trustwave Holdings, Inc.

Engine Executive Name List

Allows you to maintain a list of personal names and/or email addresses that will be used to help with detection of targeted fraud email for all incoming messages managed by this server. You can also maintain separate lists for each domain, using the Local Domain settings. For more information about this facility, see the technical reference "MailMarshal BEC Fraud Detection Basics," available from the documentation section of the LevelBlue website.

Engine Advanced options

Allows you to set options for RTF stamping and unpacking depth.

Receiver Advanced options

Allows you to set behaviors of the MailMarshal Receiver, including greeting strings, advertising of ESMTP, and other items.

Sender Advanced options

Allows you to set behaviors of the MailMarshal Sender, including ESMTP sending and deadlettering options.

Server Threads

Allows you to configure threading for optimal performance.

Templates

Allows you to override the administrative notification messages built in to MailMarshal.

Times

Allows you to set retry and expiration timeouts for the Receiver and Sender services.

Commit Scheduling

Allows you to specify times of day when configuration changes should be committed at the MailMarshal node processing servers. This functionality is designed to allow deferred commits so as to minimize impact on systems during the business day. The commit schedule is relative to the time zone of each processing server.

Product Improvement Program

Allows you to opt in or out of the Product Improvement Program. See Help for details.

To configure advanced server options:

1. In the left pane of the Management Console, click **System Configuration.**
2. In the right pane menu tree, navigate to the required option, found under Advanced System Properties, Engine Properties, or other Advanced items.
3. Specify the appropriate values. For more information about the options, click **Help**.

Copyright © 2026 Trustwave Holdings, Inc.

4. Click **Save**.

9.14.2 Advanced Settings

The Advanced Settings page of the Console (**Configuration > Advanced Settings**) allows you to manage additional detailed settings for the MailMarshal installation. These settings generally replace the Registry configuration items that were used in earlier versions. For more information see Help and LevelBlue Knowledgebase articles.

The Console also includes an Advanced Settings page for each email processing server, found under **Management > Mail Servers**.

9.14.3 Setting Up Syslog Integration

MailMarshal can send advanced information about messages and message handling to a Syslog server. Information that can be sent includes:

- Message records
- Content (message attachment) information
- Rejected message (connection blocking) details
- Quarantine Audit (message release) details.



Note: The MailMarshal Syslog integration does not handle Windows event log messages. You can forward event log information to a Syslog server using third party tools.

Before enabling Syslog in the Management Console, you must create a database to store the formatted information temporarily before it is sent. To configure this database, use the MailMarshal Server Tool (**Array Manager > Syslog Database** tab).

To configure Syslog servers and record formats:

1. In the left pane of the Management Console, click **System Configuration.**
2. Navigate to **Array Properties > Syslog**.
3. Select **Enable Syslog**, and then configure the information required to connect to the Syslog server. You can select:
    - The server name or IP address and listening port
    - The transport method (UDP, TCP, or TCP with TLS)
        - If you select TCP with TLS, the certificate of the Array Manager REST API interface is used.
    - The record format
    - The hostname and application name to include in the Syslog records
4. In the Templates section, select the types of data to be sent, and configure templates to control the data included in each record.

For more information, click **Help**.

Copyright © 2026 Trustwave Holdings, Inc.

9.14.4 Setting Up Azure Information Protection Integration

MailMarshal can scan documents protected by Azure Information Protection (AIP) Rights Management.

MailMarshal provides full support for the following (including scanning, message repacking, and viewing in the Console), provided that MailMarshal has the correct rights to read the protected content:

- Restricted-permission message (RPMSG)
- Office documents in either binary format (also known as compound files), or ECMA-376 Office Open XML format.
- Generic pfiles (files unpacked from a protected message, including images, documents, zip files, and any files supported by MailMarshal).



Note: MailMarshal does not scan or change documents delivered by direct link (where the email client does not support AIP Rights Management and the user clicks a link that retrieves the document from Azure directly). In these cases the original content is delivered over the link, and MailMarshal does not have access to this data.

Before enabling AIP in the Management Console, you must install the Rights Management Service (RMS) Client on all processing servers. The RMS Client installer is available from a link on the MailMarshal installer Prerequisites page.

To validate the presence of the RMS client:

1. In the left pane of the Management Console, click **System Configuration.**
2. Edit the properties of each server, and navigate to the Azure Information Protection tab.

To enter and validate AIP credentials:

1. In the left pane of the Management Console, click **System Configuration.**
2. Navigate to **Array Properties > Azure Information Protection**.

For more details, see Knowledgebase article Q21029, and Help for this Management Console page.



Caution: If you enter and commit incorrect details for AIP, messages that require the AIP RMS functionality will be deadlettered. If AIP RMS components are detected in a message but no AIP credentials are available, this fact is logged in the Engine log.

9.14.5 Setting Node Properties – Advanced

These options affect delivery and processing of email. If more than one MailMarshal server is included in an array, these options can be set for each server.

- Receiver Binding
- Server Host Name
- Notification Delivery

For more information about these settings, see “Customizing Settings for Nodes” on page 196.

Copyright © 2026 Trustwave Holdings, Inc.

9.14.6 Working with Array Communications

When MailMarshal is configured as an array of servers with an Array Manager and one or more other servers as email processing servers, the MailMarshal servers communicate over TCP/IP. By default, MailMarshal uses port 19001. If the Array Manager and email processing services are installed on the same server, by default the email processing services use port 19002.

You can configure these settings using the MailMarshal Server Tool, which is installed on each server. You must configure the settings on each server individually.



Note: Do not attempt to make changes in the MailMarshal Management Console application while using the Server Tool.

9.14.6.1 Changing Array Port Settings

You can change the TCP ports used by the MailMarshal services. For instance, you may want to alter the default port numbers to enhance security.

To change the port settings:

1. Log on to the server using an account with Administrator permissions.
2. Run the MailMarshal Server Tool from the MailMarshal Tools group in the MailMarshal program group.
3. *If the server is an email processing server* (not an Array Manager or standalone server):
    a. On the Node > Array page, you can change the Node Port used by the services to listen for communications from the Array Manager. When you apply this change and restart the services, MailMarshal will report the change to the Array Manager.
    b. You can also change the Array Manager port used by the services to connect to the Array Manager. This entry must match the port specified at the Array Manager.
4. *If the server is an Array Manager:* On the **Array Manager > Ports** page, you can change the port used by the Array Manager to accept connections from email processing servers and the SQM component.



Note: If you change this value, to restore full functionality you must also change the corresponding value in the SQM website configuration if installed.

9.14.6.2 Changing the Database Location

You can change the location of the MailMarshal database using the Server Tool on the Array Manager server. Because most configuration information is stored in the database, in general you should only use this option if you must change the Microsoft SQL Server on which the database is hosted.

When you create a new database, MailMarshal does not retain Spam Quarantine Management logins and related data.

To change the database location:

1. Back up the MailMarshal configuration.
2. Log on to the Array Manager server using an account with Administrator permissions.

Copyright © 2026 Trustwave Holdings, Inc.

3. Run the MailMarshal Server Tool from the MailMarshal Tools group in the MailMarshal program group.
4. If you want to move the existing database:
   a. Stop all MailMarshal services.
   b. Move the database to the new location using Microsoft SQL Server tools.
5. On the Database page, enter the new SQL Server name and database name. Click **Apply.** If necessary, MailMarshal will present options to use or recreate an existing database. *If you have moved a database and selected it,* choose **Use** and click **OK.**
6. If the Array Manager also hosts a processing node, MailMarshal will offer to rejoin the node to the array. You must complete this step either now or later.
7. MailMarshal will ask to restart services. You must complete this step either now or later.
8. Restore the MailMarshal configuration.
9. *If the installation is an array with additional processing nodes*, use the Server Tool on each email processing server to rejoin the servers to the array. See “Joining a Node to an Array” on page 196.

9.14.7 Changing Folder Locations

You can change the default location for MailMarshal logging, quarantine, message unpacking, and message queues on each email processing server using the MailMarshal Server Tool. For more information about the how these folders are used, see “Understanding MailMarshal Folder Locations” on page 36.

To change the locations of folders:

1. Using the MailMarshal Management Console, stop the MailMarshal services on the email processing server where you want to move folders.
2. Log on to the email processing server using an account with Administrator permissions.
3. Run the MailMarshal Server Tool from the MailMarshal Tools group in the MailMarshal program group.
4. On the Array Manager > Folders page and/or the Node > Folders page, change the locations. You can enter a full path relative to a local drive letter, or a partial path relative to the MailMarshal installation folder.
5. Click **OK.** The Server Tool will offer to copy files from the old locations. The Server tool will also offer to restart the MailMarshal services.
6. The Server Tool will not delete files from the old locations. You can safely do so using normal Windows procedures.



Note: You can change the location of an individual folder. For more information, see “Working with Folders” on page 155.

9.15 Using the Group File Import Tool

The MailMarshal Group File Import Tool is a command-line tool you can use to import information into MailMarshal user groups.

Copyright © 2026 Trustwave Holdings, Inc.

Run the `GroupFileImport.exe` from the MailMarshal `\InstallPath` folder. By default, the installation path is `\Program Files\Trustwave\Secure Email Gateway`.

Caution: Replacing the membership of a large group can take a significant amount of time. If you plan frequent changes to groups that are actively used in rules, consider using Connector based groups or the REST API.

To use the group file import tool:

1. Using a text editor such as Notepad, create the input file that contains the names of the groups and user email addresses you want to import. For more information, see “Group File Import Text File Format” on page 206.
2. Log onto the Array Manager computer as a member of the local Administrators group or other user account with permissions to modify the registry.
3. Open a command window and navigate to the folder where you installed MailMarshal.
4. Type the group file import command with the options you want to specify. For more information, see “Group File Import Command Format” on page 206.
5. After the users and groups are imported, close the command window.

Note: User and group information is synchronized to processing servers within a few minutes. Configuration commit is not required.

9.15.1 Group File Import Text File Format

To use this tool, create a file using a plain text editor, such as Notepad. The file contains group names followed by a list of email addresses of the users in each group. You can also use the asterisk (*) wildcard to allow address matching. The following text illustrates the file format to use:

Table 25: Group File Import file syntax

Element	Description
[New Group]	Group name
Jim@example.com	Email address
John@example.com	Email address
q*@example.com	Several email addresses specified using wildcard

9.15.2 Group File Import Command Format

Use the following syntax and options to issue the command:

```
GroupFileImport.exe [options] {-f inputfilename}
```

The following example imports user addresses from `mygroups.txt`, and merges the addresses into the group if the group name already exists.

Copyright © 2026 Trustwave Holdings, Inc.

```
GroupFileImport.exe -m -f mygroups.txt
```

Table 26: Group File Import command options

Option	Use
-h {*computer name or identifier*}	Array Manager name or IP address. Defaults to `localhost`.
-p {*IP Port*}	Array Manager port (defaults to `19001`).
-n {*text*}	Text string prefixed to all group names at import, such as *File Group:*
-m	Merge imported data. **Cautions**: If a group in the import file has the same name as an existing group, existing items in the group are not deleted. MailMarshal adds new items from the import file group. Using the command without the -m switch deletes all members from an existing group before importing the file contents.
-v	Verbose mode. Generates warnings about individual group members for troubleshooting.
-u {*user name*}	User name used to connect to the Array Manager server. Defaults to the logged-on user.
-d {*domain*}	Domain in which the user name is found.
-k {*password*}	Password associated with the user name.
-?	Prints help for the utility.

9.16 Using the Configuration Export Tool

The MailMarshal Configuration Export Tool is a command line tool that allows you to export and import MailMarshal configuration settings from a command line interface or batch file. The input and output of this command is a zip archive that contains the MailMarshal configuration information.

Note: To import a configuration saved from MailMarshal 8.2 in XML format, use the Configuration Converter Tool described in “Using the Configuration Converter Tool” on page 208.

You can use the Configuration Export tool from any system that has HTTPS access to the Array Manager and the Config Service site. Default settings assume the tool is running on the Array Manager computer. Open a command prompt to run the command.

Caution: This version of the tool has different functionality compared to earlier versions. Some options have different meanings or defaults.

9.16.1 Export Configuration Command Format

The syntax and options of the `MMExportCfg.exe` command are as follows:

Copyright © 2026 Trustwave Holdings, Inc.

```
MMExportCfg.exe -u {username} -p {password} [other options]
```

The following example imports the MailMarshal configuration from `myconfig.zip` to the local system.

```
MMExportCfg.exe -u admin -p admin -i -f myconfig.zip
```

Table 27: Configuration Export Tool command options

Option	Use
-h	Display help.
-f	Specifies the name of the file for export or import. Use the extension .zip
-d *{password}*	On export, include DKIM keys and protect them with the password. On import, import DKIM keys that are protected by the password.
-v	Show verbose information about the import or export.
-a *{URL}*	Array Manager URL. Defaults to `https://localhost:19006`.
-c *{URL}*	Config Service URL, used to log in and get a credential (JWT ticket) to access the Array Manager. Defaults to `https://localhost:19007`.
-u *{username}*	Username to authenticate. This is always a MailMarshal username, not a Windows credential, regardless of the settings for Management Console authentication.
-p *{password}*	Password to authenticate.
-i	Imports the configuration from the specified file. Without the -i option, the command **exports** the configuration.
-r	On import, replace DLL files such as Unpacker and FileType with the files from the import. If you do not include this option, the currently running copies of DLL files will not be changed.

9.17 Using the Configuration Converter Tool

You can use the Configuration Converter to update the format of a configuration file saved from MailMarshal 8.2.3 or later 8.2 release. The syntax and options of the `MMConvConfig.exe` command are as follows:

```
MMConvConfig.exe {inputfile.xml} {outputfile.zip}
```

For example:

```
MMConvConfig.exe 823Backup.xml updatedReadyToRestore.zip
```


Copyright © 2026 Trustwave Holdings, Inc.

9.18 Using the Config Service Admin Tool

The MailMarshal Config Service Admin Tool is a Windows application that allows you to manage the following items:

- Database and website connectivity settings of the Management Console
- Superusers of the Management Console and API
- Authentication method for the Management Console. Available methods include MailMarshal authorized users/passwords, Windows Authentication, or SAML based Single Sign On.
- Windows groups to check for allowed Windows users of the Management Console (if Windows Authentication is configured).

To use the tool, log on to the server hosting the Management Console website, using a Windows account with administrative permissions (for example, as a member of the Windows administrator group on the system). From the Start menu select **MailMarshal Config Service Admin Tool**, or navigate to the `Config Service` subfolder in the MailMarshal installation folder, and run `SegCfgServiceAdminTool.exe`. For more information, see Help for the tool.

Copyright © 2026 Trustwave Holdings, Inc.

10 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. If an organization generates a large number of these cases, the email administrator may not have the time required to review them. This situation is likely to arise with messages that MailMarshal has classified as spam.

MailMarshal provides several options that allow the administrator to delegate the responsibility for reviewing these messages and taking action:

- Departmental administrators or help desk personnel can have permission to process the messages in selected quarantine folders, using the MailMarshal Management Console.
- Each email user can receive a daily summary of their incoming messages that have been quarantined, through MailMarshal digest emails.
- Each email user can have permission to review and release messages quarantined in one or more folders, through the MailMarshal Spam Quarantine Management Website. This facility is specifically designed to allow users to review messages that have been classified as spam, but it can be used for other classifications. It also allows each user to refine the spam classification by maintaining personal lists of safe and blocked senders.
- Where a policy requires a small number of messages to be held for review, users can receive notice of each message and release it by email using the MailMarshal Message Release external command. For more information, see “Using the Message Release External Command” on page 215.
- Actions taken on messages by any user are recorded and can be reviewed using the Quarantine Audit feature in the Management Console.

10.1 Setting Up Console Access

MailMarshal controls access to the features of the Management Console through accounts managed in the Console or the Config Service Admin Tool. For more details see “Managing Authorized Users” on page 66.

10.2 Setting Up Spam Quarantine Management Features

The MailMarshal 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 rules to help determine whether email sent to that user is spam.

For information about setting up the Spam Quarantine Management Website, see “Installing and Customizing Web Components” on page 57.

Copyright © 2026 Trustwave Holdings, Inc.

10.2.1 Spam Quarantine Management Windows

The Spam Quarantine Management Website includes the following pages:

Log In

Allows a user to enter an email address and password to log in to the Spam Quarantine Management Website. Also allows a user to request a login and to request a new password. MailMarshal only uses this page if you configure the site to use authentication by email address and password ("forms" authentication).

Home

Allows a user to view a list of email blocked since their last visit, and summary charts of blocked and good email (if allowed by the administrative settings).

Blocked Mail

Allows a user to review a list of email quarantined in one or more folders. The user can see message details and release or delete each message. The user can also add the sender address to the blocked or safe senders list (if allowed by the administrative settings). If more than one folder is available through this site, the page shows a list of folders the user can review.

Message Details

Allows a user to view the initial part of the body and additional details of a message from the list of blocked email. The user can release the message or delete the message, and add the sender to blocked or safe senders.

Manage Senders

Allows a user to add, edit, or delete entries in lists of safe and blocked email addresses. MailMarshal uses these lists in the rule condition "Where sender is/is not in recipient's safe senders list" and "Where sender is/is not in recipient's blocked senders list."

User Settings

Allows a user to configure site and address options.



Note: Some options can be globally enabled or disabled by the administrator (using options on the Administrator tab of the site).

- Set the site look and feel.
- Add or delete entries in a list of email addresses that they can manage using this login (if allowed by the administrative settings). Before adding a requested address to the list, MailMarshal requests confirmation by sending a message to the email address. The user must click a link in the message and confirm the request.
- Delegate the power to review their blocked email to one or more other users. The delegates will also be able to edit the user's blocked and safe senders lists. The delegates can choose

Copyright © 2026 Trustwave Holdings, Inc.

which user's email to review using a list at the top of the page. Depending on the site authentication setting, delegation is by email addresses or Windows user names.

- Choose to receive, or not receive, specific digests (if permitted by the global settings of each digest).

Change Password

Allows a user to change the password associated with their login (email address) for this site. MailMarshal only uses this page if you configure the site to use authentication by email address and password.

Administrator

Allows Site Administrators to perform configuration and administration functions for the Spam Quarantine Management site:

- configure site settings
- globally enable and disable use of site features including the charts, safe senders and blocked senders, email address management, folder counts, and "all folders" view.
- delete users
- view and act on blocked mail for any user
- edit the safe, blocked, delegate, and owned email addresses for any user

Help

Each page includes a link to a Help window that provides additional information about fields and functions.

10.2.2 Setting Up Folders and Templates

The primary use of the Spam Quarantine Management Website is to allow users to review messages that MailMarshal has quarantined as spam. You can configure the site to manage one or more folders used for this purpose. You can also configure the site to manage folders that are used for other purposes.

Each folder managed by the Spam Quarantine Management Website can contain either messages sent to local users or messages sent by local users, but not both.

To set up folders to manage spam with the Spam Quarantine Management Website:

1. Create or edit a MailMarshal folder. See "Using Folders and Message Classifications" on page 154.
2. In the folder properties, select (toggle on) **Enable End-user Management for this folder.**
3. Choose the setting **Folder is used to manage messages addressed to a user**.
4. *If you want each user to receive a digested notification* of messages addressed to or from them that have been quarantined in this folder, create a message digest that includes the folder. See "Setting Up Message Digests" on page 213.

Copyright © 2026 Trustwave Holdings, Inc.

5. Repeat Steps **1** to **4** for each folder you want to set up for Spam Quarantine Management.

10.2.3 Setting Up Message Digests

MailMarshal allows you to send email summaries to users, notifying them about messages addressed to or from them that MailMarshal has quarantined. When the SQM website is installed, users can release the messages directly from the digest email. Digests are often used for the same folders that are available for end user management in the SQM website, but you can also create digests to allow message releasing for other folders.

A digest only lists messages that have not been included in a previous digest.

A message digest can

- Include information about messages in one or more folders
- Include or exclude messages from digesting, by checking user groups
- Be generated using one or more schedules. Each schedule causes the digest to be generated at a specified time on one or more days each week
- Use a specified email template. To learn more about templates, see “Creating Digest Templates” on page 144.
- Send digest emails to the recipient or sender of the original messages.
- Send digest emails to each user with undigested email in the folder, or send all digest emails to a specified address.



Note: Digests that send all digest emails to a specified address can be used for both inbound and outbound email.

- Allow users to subscribe or unsubscribe from the digest using the SQM website or release web-page.

To work with message digests in the Management Console, select Policy Elements from the left pane menu tree and then select Message Digests from the right pane menu.

10.2.3.1 Creating Message Digests

You can create as many digests as your policy requires.

To create a message digest:

1. On the toolbar, click **Add**.
2. On the Message Digest panel, specify the appropriate values. The Schedule, Folders and Notification tabs (buttons) allow you to set advanced features. Advanced features include multiple schedules, selection of email to digest by user group, and the recipient of digest emails (original recipient, original sender, or a single address for all digests). For more information about fields and workflow, click **Help**.
3. Click **Save.**

Copyright © 2026 Trustwave Holdings, Inc.

10.2.3.2 Editing Message Digests

You can edit the name and features of a digest.

To edit a message digest:

1. Double-click the digest name in the right pane of the Management Console to view its properties.
2. On each field and tab, specify the appropriate values. For more information about fields and workflow, click **Help**.
3. Click **Save.**

10.2.3.3 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 Management Console.
2. Click the **Delete** icon in the toolbar.

10.2.4 Setting Up Rules

MailMarshal places email in quarantine folders through rule action.

To set up spam Quarantine rules:

1. Create MailMarshal rules to move spam messages into each folder you have created. If you are using the default configuration provided with MailMarshal, rules are included in the Spam policy group to move spam messages into several folders.
2. Within the rule or rules, use the condition “Where the sender is in the recipient’s allow list.” Configure the rule so that messages that meet this condition are not quarantined as spam.
3. Within the rule or rules, use the condition “Where the sender is in the recipient’s block list.” Configure the rule so that messages that meet this condition are quarantined as spam.



Note: If you are using the default configuration provided with MailMarshal, the rules included in the Spam policy group use these conditions.

The user safe and block list conditions use the Safe Senders and Blocked Senders lists maintained within the Spam Quarantine Management website. If the SQM website is not in use, or if you choose to disable these lists (using the Administrator access to the SQM website), then these rule conditions will have no effect.

4. When a user releases a message from the SQM website, MailMarshal continue processing the message as specified in the rule that moved the message to the folder. For more information, see “BCC a copy of the message” on page 117.

10.2.5 Setting Up Spam Quarantine Management for Other Folders

You can configure any MailMarshal folder to be managed through the Spam Quarantine Management Website.



Note: Each folder can be used for inbound or outbound messages, but not both.

Copyright © 2026 Trustwave Holdings, Inc.

To set up folders to manage other messages with the Spam Quarantine Management Website:

1. Create or edit a MailMarshal folder. See “Using Folders and Message Classifications” on page 154.
2. Select (toggle on) the setting **Enable End-user Management for this folder.**
3. Select either **Folder is used to manage messages addressed to a user** or **Folder is used to manage messages addressed from a user** as appropriate.



Tip: When you create rules to quarantine messages in these folders, be sure to direct **inbound** (“to a user”) **and outbound (**“from a user”**)** messages to the **appropriate folders.** This setting is used to determine the local user who will be able to manage the messages through the Spam Quarantine Management website.

To set the recipient for digests, configure the “messages are treated as” setting in digest properties.

4. *If you want each user to receive a digested notification* of messages (addressed to or from them) that have been quarantined in this folder, create a message digest that includes the folder. See “Setting Up Message Digests” on page 213.
5. Repeat Steps **1** to **4** for each folder you want to set up for Spam Quarantine Management.

10.3 Using the Message Release External Command

Some MailMarshal 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.

To use automatic message release:

1. Create or modify a MailMarshal rule which moves certain messages to a folder.
2. In this rule, include a rule action which sends a notification message. The body of this message must contain the variable `{ReleaseProcessRemaining}` or `{ReleasePassThrough}`.
   - The `{ReleaseProcessRemaining}` variable causes the message to be processed through additional rules, as specified in the Release Action of the rule that quarantined it. For more information, see “BCC a copy of the message” on page 117. This option is more secure and recommended.
   - The {`ReleasePassThrough}` variable causes the message to be queued for delivery with no further processing of rules. See the pre-configured template Automatic Message Release Outbound for an example.



Note: The message template *must* include a plain text message body. It may include a HTML body as well.

The From address must be one which guarantees that replies will pass through MailMarshal. The address need not be valid but it must be well-formed.

To process message release requests, create a MailMarshal rule similar to the following:

Copyright © 2026 Trustwave Holdings, Inc.

```
Where addressed to MessageRelease@Release.example.com
Run the external command Message Release
And write log message(s) with Release Requests
And delete the message
```

The message classification “Release Requests” is pre-configured.

Automatic Message Release should be used sparingly as it tends to defeat the purpose of MailMarshal.

If MailMarshal is used in an array with separate Array Manager and processing servers, the Message Release external command must run using a Windows credential that the Array Manager can validate. You can enter specific account credentials for the Message Release external command, using command line parameters in the External Command definition. See “Message Release Options.”



Tip: If the account is not the local Administrator, you may need to grant the account full permission over the MailMarshal Registry location. (Adding an account to the “Administrators” group is not sufficient.).

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.

10.3.0.1 Message Release Options

The Message Release external command has the following syntax:

```
MMReleaseMessage [-u username] [-p password] [-d domain] [-r recipient] [-
l true] [-v true] {MessageName}
```



Note: `{MessageName}` is a MailMarshal variable. The braces are part of the variable syntax. You must include this literal string in the command parameters.

To use the options, edit the external command definition. In the properties, change the parameters field to include the required options.

The options are further described as follows:

```
-u {username}
-p {password}
-d {domain}
```

- Use these options to run the external command as a specific Windows user. This functionality may be required on recent versions of Windows Server with enhanced security configuration.



Note: If you use these options, you must include the password value.

`-v` `true` verbose logging for debugging purposes (Must have the argument `true`)
`-l` `true` leave message in folder (Must have the argument `true`)
`-r` send only to named recipient

Copyright © 2026 Trustwave Holdings, Inc.

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 true` (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.

Copyright © 2026 Trustwave Holdings, Inc.

11 Reporting on MailMarshal Activity

The **Marshal Reporting Console** application allows you to generate reports based on the information MailMarshal logs as it processes email messages. You can choose from a wide range of reports covering email throughput, specific content, and threat information. You can produce both overall summaries and per-user information.

The Marshal Reporting Console is based on SQL Server Reporting Services, and offers scheduled generation and automatic delivery of reports. For more information about this application, see the LevelBlue website or contact LevelBlue.

Message history **i**nformation can also be delivered to a **Syslog** server. For more information, see “Setting Up Syslog Integration” on page 202.

Auditing of MailMarshal **policy changes** is available through the Audit History item in the MailMarshal Management Console. For more information, see “Change Auditing” on page 66.

Auditing of changes to Authorized Users of the Management Console is available through the User Account Audit item in the MailMarshal Management Console.

Auditing of message release activity by users and other actions on quarantined messages is available through the Quarantine Audit item in the MailMarshal Management Console.

11.1 Data Retention and Grouping

The data available for reports in the Marshal Reporting Console, and grouping of certain items, is configured through the MailMarshal Management Console.

To configure reporting options:

1. In the left pane of the Management Console, click **System Configuration**. In the right pane tree, expand **Array Properties** and click **Reporting**.
2. When you have completed changes to Reporting options as described in the next sections of this chapter, click **Save** and then commit the MailMarshal configuration to effect the changes.

11.1.1 Configuring Data Retention

You can adjust the length of time MailMarshal retains logging records. Best practice is to retain enough data to allow reporting on several months of email traffic. You can also reduce the size of your MailMarshal database by reducing the retention time.

If you archive messages in a MailMarshal folder for longer than the logging retention time, MailMarshal will retain basic database records about each archived message for as long as the archives are retained. This information is necessary to allow viewing of the messages in the Console. For more information about backing up and restoring messages in quarantine folders, see the LevelBlue Knowledgebase.

To configure your reporting data retention period, in the **Retain** field, enter a number of days. Click **Save.**

Copyright © 2026 Trustwave Holdings, Inc.

11.1.2 Configuring Reporting Groups

Information about spam and viruses is likely to be logged in varying classifications and folders. To allow unified reporting on these categories, MailMarshal allows you to specify the folders and classifications you are using for each of these types of content. These groups affect the display on the Dashboard page of the Console, as well as the Spam Overview report, the Virus Overview report, and the two virus detail reports available in the Marshal Reporting Console.

To configure the reporting groups:

1. In the left pane of the Management Console, click **System Configuration**. In the right pane tree, expand **Advanced System Properties** and click **Reporting Groups**. Each of the three available Groups is shown as a tab.
2. To change the items included in a group, navigate to the tab for that group. Select the items you want to include. When you have configured all groups, click **Save**.



Note: Be sure to select only the folders and classifications that relate to the purpose of the group.

Copyright © 2026 Trustwave Holdings, Inc.

Appendix A: Wildcards and Regular Expressions

MailMarshal supports a simple wildcard syntax when you enter several types of information including local domains and user groups.

MailMarshal also uses a full Regular Expression syntax for matching and substitution in Header Rewrite rules.

A.1 Wildcard Characters

- MailMarshal allows wildcard entries in the following contexts:
- Local domains. See “Running the Configuration Wizard” on page 48.
- User and Group matching for policy groups and rules. See “Understanding User Matching” on page 92.
- Receiver HELO name matching. See “Where sender's HELO name is/is not criteria” on page 110.
- The Console search and filtering options. See “Using the MailMarshal Console for Email Management” on page 167.
- BTM exclusions. See “MailMarshal Properties – Advanced” on page 200.
- Outbound TLS domains. See “Securing Outbound Communications” on page 200.

In each of these types of entry, MailMarshal supports this syntax:

Table 28: Wildcard syntax

Character	Function
`*`	Matches any number of characters
`?`	Matches any single character
`[abc]`	Matches a single character from a b c
`[!abc] or [^abc]`	Matches a single character except a b or c
`[a!b^c]`	Matches a single character from a b c ! ^
`[a-d]`	Matches a single character in the range from a to d inclusive
`[^a-z]`	Matches a single character not in the range a to z inclusive

Copyright © 2026 Trustwave Holdings, Inc.

The table below gives some examples of results of the wildcard syntax.

Table 29: Wildcard example results

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 [ ].

A.2 Regular Expressions

MailMarshal uses regular expressions in header matching and rewriting rules. For more information about these rules, see “Content Analysis Policy” on page 88. MailMarshal also uses regular expressions in category scripts. For more information about category scripts, see the technical references “MailMarshal Anti-Spam Configuration” and “MailMarshal Advanced Anti-Spam Configuration,” available from the MailMarshal support page at LevelBlue.com.

MailMarshal 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 Knowledgebase article Q10520.

This appendix provides limited information about some commonly used features and some extensions specific to MailMarshal.

Note: MailMarshal also uses Regular Expressions in TextCensor scripts. This feature uses a different Regular Expression engine with very similar syntax to that described in this section. For more information and a link to detailed documentation, see “Anchored Regular Expressions” on page 133.

Copyright © 2026 Trustwave Holdings, Inc.

A.2.1 Shortcuts

The arrow to the right of each field on the Expressions tab of the header rule panel provides access to some commonly used Regular Expression features.

Table 30: Regular Expression shortcuts

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. This expression will be saved for use within the substitution field.
Or	|	The field will be matched if it matches either the expression before the | or the expression after the |.
0 or more matches	*	The expression before the * will be matched if it is repeated any number of times, including zero.
1 or more matches	+	The expression before the + will be matched if it is repeated at least once.
Repeat	{ }	Enter a number or two numbers separated by a comma within the braces. The expression before the braces will be matched if it is repeated the number of times specified. See “Repeat Operators * + ? {}” on page 223.
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.

A.2.2 Reserved Characters

Some characters have special meanings within regular expressions.

A.2.2.1 Operators

The following characters are reserved as regular expression operators:

* . ? + ( ) { } [ ] $ \ | ^ <

Copyright © 2026 Trustwave Holdings, Inc.

To match any of these characters literally, precede it with \

For example, to match `marshal.com` enter `Marshal\.com`

A.2.2.2 Wildcard Character .

The dot character (.) matches any single character.

A.2.2.3 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.

A.2.2.4 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).

A.2.2.5 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

A.2.3 Examples

The following sections show examples of matching and substitution strings.

A.2.3.1 Matching

The expression

Copyright © 2026 Trustwave Holdings, Inc.

```
(.+)@(.+)\.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

A.2.3.2 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.

A.2.4 Map Files

MailMarshal 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 substitutes the second value. If the search expression does not match the first value in any line, MailMarshal 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.

A.2.4.1 Map file

```
john@domain.co.uk,                                    john@domain2.co.uk
peter@domain.co.uk, peter@host1.domain.co.uk
```

A.2.4.2 Search expression

```
(.+)@domain\.co\.uk$
```

A.2.4.3 Lookup key

```
$1@domain.co.uk
```

A.2.4.4 Sample results

The following table shows the matching addresses when the sample mapping file above is used.

Table 31: Map file example results

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

Copyright © 2026 Trustwave Holdings, Inc.

Appendix B: Third Party Extensions

MailMarshal supports integration with a number of third party products that extend MailMarshal scanning and filtering capabilities. These products include virus scanning software and image analysis software.

B.1 Image Analyzer

Image Analyzer is a third party deep image analysis product that has been fully integrated into the MailMarshal content scanning engine. Integration with Image Analyzer allows MailMarshal to assess the content of images that pass through the email gateway. For usage details, see “Where the attached image does/does not/may match image category” on page 102. LevelBlue also provides integrated licensing for this product.

Because MailMarshal unpacks the content of a message, extracting the attachments and the content inside archive files, Microsoft Word documents, and other packed formats, Image Analyzer can scan the image content from all components of the target message.

Image Analyzer can be used to check for a variety of image content, including pornography and QR codes. Image Analyzer uses a variety of techniques in its analysis. It is important to note that detection of image content is not an exact science, and the level of technology available today means that a few images may be undetected or falsely detected. A number of control settings can be selected when creating a rule for image analysis, to help tune the results of the analysis.

B.1.1 Why Would I Use Image Analyzer?

The primary goals for organizations deploying image analysis technology are to protect against malicious external linking through QR codes, to reduce legal liability and to ensure that company reputation is not compromised. Image Analyzer allows your organization to utilize leading technology, and provides evidence of due diligence in protecting your employees from accessing malicious links or receiving material that may be offensive or in some cases illegal. Executives in some countries can be held legally liable for not exercising due diligence in preventing material of this nature from entering or being stored on their systems.

Many organizations today are blocking all image content entering their organization to ensure that offensive material cannot enter. However, blocking all images can prevent the transmission of images that are required for business purposes.

Image Analyzer allows the organization to permit email transfer of legitimate images, and also to meet its legal obligations of due diligence and its more general moral obligations of protecting its employees from offensive material being delivered to them over a medium that they have no control over.

B.1.2 What Results Can I Expect From Image Analyzer?

MailMarshal 10.1 and above includes a new generation of Image Analyzer. Image Analyzer scans each image based on its visual features using a neural network. Image Analyzer has tested their

Copyright © 2026 Trustwave Holdings, Inc.

technology with a wide range of image content that typically travels the Internet. The published results of this testing show:

- Image Analyzer detects 90% of commercial pornographic images with near-zero false positives.
- Image Analyzer detects greyscale and cartoon sexually explicit images with high reliability.

These results compare favorably with other products on the market.

B.1.3 How Does Image Analyzer Address the Issues?

Although no technology can guarantee 100% protection against inappropriate image content, use of Image Analyzer can help in several ways.

- Use of Image Analyzer can help to protect against phishing and other malicious attacks by detecting QR codes.
- Use of Image Analyzer can help to reduce liability by showing due diligence in providing an appropriate environment.
- The policy based functionality of MailMarshal allows social education on the issue of appropriate content within an organization. Individuals who exchange inappropriate material tend to do so repeatedly. MailMarshal can send a notification to the sender when it detects inappropriate content. Even if MailMarshal does not detect every instance of the material, the individuals will be educated that the content of email is being analyzed and monitored. The risk of action being taken, or social embarrassment, rapidly increases. Most users will cease to send material that they know is not acceptable under your organization's policy.

B.2 Virus Scanning Software

MailMarshal provides high-throughput DLL interfaces to a number of well-known virus scanning products. In addition to a DLL interface, MailMarshal also provides integrated licensing and a customized upgrade component for the Bitdefender, McAfee, and Sophos scanners. For usage details, see "Configuring Antivirus Scanning" on page 54 and "Stopping Viruses and Malware" on page 75.

Anti-virus software is considered a basic requirement for secure business networks. Integration of anti-virus scanning with MailMarshal allows checking for email viruses at the network boundary. This capability provides an added layer of protection beyond what desktop scanners can provide.

Copyright © 2026 Trustwave Holdings, Inc.

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.

blended threat
Security threat to a network using multiple vectors (for instance, a malicious URL sent by email).

component
Individual part of a MailMarshal implementation that performs a specific function. For example, an email processing server, Array Manager, or database is a MailMarshal component.

computer name
A name that uniquely identifies a computer on a network. The computer name cannot be the same as any other computer or domain name on the network. The network uses the computer name to identify the computer and to allow other users to access the shared resources on that computer.

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.

Copyright © 2026 Trustwave Holdings, Inc.

distinguished name
An address format used to locate and access objects in an X.500 directory using the LDAP protocol. This format specifies the complete path to the object through the hierarchy of containers in a domain. Each distinguished name is unique. For example, a user object with the common name J. Doe in the organizational unit container called Users on the domain marshal.com might be represented as follows:
`CN=JDoe,OU=Users,DC=Marshal,DC=com`

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
See Domain Name Service (DNS).

DNS blocklist
A service that provides an automated response through the DNS protocol. DNS blocklists typically attempt to list email servers that are associated with spamming, open relays, or other unacceptable behavior.

Domain-based Message Authentication, Reporting & Conformance (DMARC)
An email validation standard and system based on SPF and DKIM checks. The owner of a sending domain sets a policy that defines validation methods used by their domain, and suggests how recipients should deal with messages that fail validation. The recipient returns reports about messages and actions to the sending domain.

DomainKeys Identified Mail (DKIM)
A method of digitally signing an email message. Public keys used to verify the signature are retrieved from special DNS records.

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.

Copyright © 2026 Trustwave Holdings, Inc.

Extensible Markup Language (XML)
A data tagging language that permits the storage and interchange of structured data.

fault tolerance
The ability of a product to respond to a catastrophic event (fault) that ensures no data is lost and that any work in progress is not corrupted.

firewall
A security system that is placed between the Internet and the private network of an organization, or within a network, and only passes authorized network traffic.

folder classification
An entry indicating a quarantine folder name written to the MailMarshal database when a file is moved to a quarantine folder. MailMarshal creates the database entry automatically.

hyperlink
An emphasized portion of text on a window that, when clicked, opens another document or window.

IIS
See Microsoft Internet Information Services (IIS).

Lightweight Directory Access Protocol (LDAP)
A network protocol designed to work on TCP/IP stacks to extract information from a hierarchical directory such as X.500. It is useful for searching through data to find a particular piece of information. An example of an LDAP directory is the Active Directory in Windows 2003 or later. Objects in an LDAP directory are identified by their distinguished names.

local area network (LAN)
A group of computers in the same place that are connected and typically have the same network operating system installed. Users on a LAN can share storage devices, printers, applications, data, and other resources.

mailbox
A disk storage space assigned to a user account to receive incoming email messages.

Management Console
Web-based interface that allows you to edit email policy, configure email delivery and server settings, monitor email traffic and manage quarantined email. Intended to be used by email administrators, managers, and help desk personnel. This interface replaces the legacy Configurator, Console, and Web Console from Trustwave SEG 8.X and below.

MDAC
See Microsoft Data Access Components (MDAC).

message classification
Classification action defined in a rule as `Write log message with x`.

Copyright © 2026 Trustwave Holdings, Inc.

Microsoft Data Access Components (MDAC)
A set of network libraries and programming interfaces designed to allow client applications to connect to data providers such as SQL Server databases.

Microsoft Internet Information Services (IIS)
A Web server application for Windows operating systems.

Microsoft Management Console (MMC)
A common interface designed to host administrative tools for networks, computers, services, and other system components.

Multi-Purpose Internet Email Extensions (MIME)
A standard that permits transmission of content other than text through SMTP email.

Microsoft SQL Server Desktop Engine (MSDE)
A freely distributable limited version of SQL Server 2000. Note that MSDE is no longer supported by MailMarshal.

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.

Copyright © 2026 Trustwave Holdings, Inc.

reputation service
A service that provides an automated response that classifies the source of an email message. Reputation services are usually implemented as DNS blocklists.

scalability
Ability to distribute loads across multiple servers, allowing for greater accessibility and balanced traffic.

Sender ID
A standard for validation of the source of an email message, based on special DNS records. Typically used for anti-phishing checks.

Sender Policy Framework (SPF)
A standard for validation of the source of an email message, based on special DNS records. Typically used for anti-phishing checks.

service account
In Windows NT it is a user account that a service uses to log on to Windows NT. The account must have the specific rights and permissions required by that service.

Simple Mail Transfer Protocol (SMTP)
A member of the TCP/IP suite of protocols. The standard governing email delivery over the Internet.

SMTP
See Simple Mail Transfer Protocol (SMTP).

Spam
Unsolicited email messages, usually of a commercial nature.

SpamBotCensor
A proprietary spam detection technology incorporated in MailMarshal. SpamBotCensor leverages the message analysis tools of SpamCensor to efficiently identify spam that is generated by botnets.

SpamCensor
A proprietary spam detection technology incorporated in MailMarshal. SpamCensor includes a multi-faceted message analysis tool and regular definition updates.

SpamProfiler
A proprietary spam and malware detection technology incorporated in MailMarshal. SpamProfiler is a signature based system that operates during message reception and includes real-time updating.

Spam Quarantine Management Website
Interface that allows a user to review and release their email messages that MailMarshal has quarantined.

split message
A message for multiple recipients that MailMarshal divides into copies. MailMarshal processes each copy differently, according to the rules indicated for a specific recipient.

Copyright © 2026 Trustwave Holdings, Inc.

spoofing
Disguising the sender address of an email message to make it appear as though it is from another person, usually for malicious reasons.

SQL Express
A freely distributable limited version of SQL Server.

SQL Server
The Microsoft enterprise database server software.

Structured Query Language (SQL)
A programming language used to retrieve information from a database.

TextCensor
The lexical analysis engine included in MailMarshal. TextCensor allows you to scan email messages and attachments for complex text content, using Boolean and proximity operators and numerical weighting.

Transport Layer Security (TLS)
A protocol intended to secure and authenticate communications (such as email) across public networks by using data encryption.

wildcard character
A character in a search pattern that represents a number of arbitrary characters within the text being searched.

X.500
A global, hierarchical directory service. For example, a domain controller hosting Active Directory on a network running Windows 2003 or later provides an X.500 directory service.

XML
See Extensible Markup Language (XML).

Copyright © 2026 Trustwave Holdings, Inc.

Index

A

Accept message 120
Acceptable Use Policy 70, 141
Accounts 81, 100, 107, 111, 191
Actions. *See* Rule Actions
Active Directory 53, 126
Adaptive allow list 79
Add message users 115
Administrative notifications 49, 74, 143
Administrator email addresses 49
Advanced options 200
Alert History 175
Aliases, email 191
Anti-Malware 76
  Supported software versions 38
Anti-relaying 70, 77, 99
Anti-Virus 76
  Supported software versions 38
Archiving 218
Array Manager 28, 42, 204
Array of servers 27, 195
Array options
  Delivery 190
  Managing nodes 195
Attachment fingerprints 101, 156
Attachment parent 102
Attachment size 105
Attachments
  Checking name 101
  Checking parent type 102
  Checking size 105
  Checking text 138
  Checking type 100
  Counting 105
  Scanning for viruses 97
  Stripping 116
  Unpacking depth 201
  Valid fingerprints 101, 115
Attack prevention 81
Azure Information Protection 203

B

Back up
  Configuration 181
  Folders 218
  Messages 218
  TextCensor scripts 140
Bandwidth required 104
BCC 117, 121, 122
Best practices 76, 93, 141, 191
Blended Threats 116
Block receipt 120
Blocked Hosts 80
Boolean operators 131

C

Category scripts 108
Certificates
  TLS 198
Classifications 114, 122, 154
Commit configuration 66, 168, 195
  Scheduling 201
Conditions. *See* Rule Conditions
Configuration
  Back up and restore 181
  Importing and exporting 207
  MailMarshal properties 65
Configurator, MailMarshal 63
Connection Policy 88
Connectors 126
Console, MailMarshal
  Understanding 67
Content Analysis Policy 88
Continue Processing Rules 121
Copy the message 114

D

Daily administration 166
Dashboard 167
Data retention 218
Database
  Changing location 204
  Size 218
Date formatting 153
Dead Letter Policy 88
Dead Letters

Copyright © 2026 Trustwave Holdings, Inc.

Causes 98, 116, 164, 165
Delegating
Console Access 210
Quarantine management 210
Spam management 210
Delete message 119, 123
Delivery, email 186, 189
Deployment scenarios 24
DHA attacks
Configuring attack prevention 84
Understanding 83
Dial-Up 193
Digest templates 144
Directory 205
Directory connectors 53, 126
Disclaimers. *See* Message stamps
Distributed enterprise 28
DKIM 109
DMZ 28
DNS 38, 50, 52, 62, 190
DNS blocklists 78
DoS attacks
Configuring attack prevention 82
Understanding 81

E

Eicar.com 55
Email
Restricting incoming 82
Securing inbound 199
Securing outbound 200
Email batching 192
Email content policies 70
Email headers
Matching 107
Rewriting 116
Email history 173
Email messages
Forwarding 169
Processing logs 170
Processing manually 172
Releasing manually 172
Retention 170
Viewing 169
Email policy
Default 86
Understanding 88
Viewing and printing 124
Email policy elements 125
Email processing server
Adding or deleting 195
Changing array port settings 204
Email transport policies 70
Engine, MailMarshal 19
Enterprise installation 28
ESMTP
Authentication 81, 100
Connection 110
Spoofing criterion 100
Event Log 177
Exporting
Configuration 181
TextCensor scripts 140
External commands
Configuring 163
Message release 215
Rule action 115
Rule condition 107

F

Fallback host, email delivery 186
False positives
Spam 210
TextCensor scripts 141
File extension 101
File name 101
File type signatures, custom 101
File types 101
Filtering email 70
Firewall 53, 186, 190
Folders
And virus scanning 55
Archive 168, 169
Compression of 35, 36, 37
Dead Letter 165, 168
Default permissions 157
Default security 157
Locations 36, 205
Logging 37
Permissions 158
Quarantine 37
Queues 36, 37
Searching 174
Security 158

Copyright © 2026 Trustwave Holdings, Inc.

Setting up Spam Quarantine Management 212
Unpacking 37
Using 154
Viewing contents 168

G

Goto action 119

H

Header Matching
Map Files 224
Header matching 107
Header rewriting
Map files 224
Order of evaluation 163
Rule action 116
Headers, email
Altering 160
Deleting 163
Inserting 163
Matching 159
Rewriting 160
HELO
Incompatibility with TLS 198
History. *See* Alert History, Email History
HTTPS 73

I

Image Analyzer 102, 225
Importing
Configuration 181
TextCensor scripts 140
User Groups 205
Users 53
Inbound communications
Securing with TLS 199
Installation
Standalone server 41
Installation options 24
ISP 50, 51, 186, 190

K

Keys, MailMarshal license
Entering 180
Invalid 179
Requesting 180
Required 179

L

LDAP
Configuring connectors 126
Creating connectors 53
License key. *See* Keys
Licenses
Managing 179
Licensing 179
Managing licenses 179
Requesting license keys 180
Reviewing installed licenses 179
Load Balancing 28, 186, 195
Local Archiving 168
Local domains
Configuring 49, 183
Delivery 197
Spoofing 99, 100
User matching 92
Localhost 27
Logging
Classifications 114, 122
Daily log files 178

M

Mail Recycle Bin 168, 170
Malware 75
Malware scanners
Configuring 75
Installing and configuring 54
Malware scanning 70
Management Console 63
McAfee for Marshal 75
Message holding 119
Message parking 119, 168
Message release 215
Message size 104, 109
Message stamps 115, 147
Message templates 142
Move the message 117, 123
MX record 26, 52, 62, 183

N

Node. *See* Email processing server
Notification message 114, 122
Notifications 97, 114, 122, 142, 163
Number of attachments 105
Number of recipients 105

Copyright © 2026 Trustwave Holdings, Inc.

O
Open relay. *See* Anti-relaying
Order of evaluation 116
Outbound communications
Securing with TLS 200

P
Parameters
Message Release 216
Pass message through 123
Pass message to rule 119
Performance Monitor 178
Policy groups
Creating 89
Order of evaluation 123
POP3 . . . . . 184, 191
Ports. *See* TCP ports
Postmaster. *See* Administrative notifications
Prerequisites 40
Properties configuration 65
Properties, Node 65
Proxy settings 74
PTR lookups 80

Q
Quarantine 173
Quarantine Audit 175, 210
Quarantine Management 210
Queued domains 168
Queued messages 168

R
Receiver binding 197
Receiver threads 197
Receiver, MailMarshal 19
Refuse message 120
Regular expressions 159, 221
Relay domain 184
Relay server 53, 186
Relaying
See also Anti-Relaying
Allowing 77, 110, 111, 120
Blocking 70
Defined 77
Release Message 173
Reports
Classifications 114, 122
Reputation services 78, 111
Restore
Configuration 181
Routing, email
Rule based 118, 122
RTF message stamping 148
Rule actions
Connection Policy 120
Content Analysis Policy 112
Rule conditions
Connection Policy 109
Content Analysis Policy 94
Dead Letter Policy 112, 121
Rule user matching 90, 92, 93
Rules
Creating 90
Global header rewriting 159
Order of evaluation 123
Receiver. *See* Connection Policy
Spam Quarantine 214
Standard. *See* Content Analysis Policy
URLCensor 72
Rulesets. *See* Policy groups

S
Schedules
Folder 119
Policy groups 89
User group reload 53
Searching
Email history 174
Folders 174
Securing
Inbound communications 199
Outbound communications 200
Sender ID 99, 100
Sender, MailMarshal 19
Sender's IP address 106, 107, 110
Server health 166
Server name 197
Server statistics 167
Server threads 201
Server, Email processing 195
Set message routing 118, 122
Signatures. *See* Message stamps
SMTP 27
SMTP Authentication 187

Copyright © 2026 Trustwave Holdings, Inc.

Spam 70, 71, 105, 108, 210, 214
Spam Quarantine Management 57, 68, 210
SpamCensor 73, 95
SpamProfiler 72, 95
SPF 110, 121
Spoofing 98, 99, 100
Stamp message 115
Standalone server 26, 41
Status page 167
Storage requirements 218
Subject line 77, 116, 138
Syslog 202

T

TCP ports
- 25 . . . . . 26, 27
- 97 27
- 110 26
- 19001 28

Templates
- Administrative 143
- Digest 144, 212
- Notification 114, 122, 143

Terminal actions 112, 119, 123
TextCensor scripts
- Editing 139
- Rule condition 100
- Scoring 136, 139
- Testing 142
- Understanding 130

Timeouts, email delivery 201
TLS 107, 111, 112
- HELO incompatibility 198
- Managing keys and certificates 198
- Working with certificates 198

TLS Certificate Wizard
- Supported operations 198

Today Page 167
Tools, MailMarshal 68

U

UDP 50, 190
Uninstalling MailMarshal 61
Upgrading MailMarshal 60
URLCensor 72
User groups ??–. . . . . 129, ??–130
User Matching. *See* Rule User Matching
Users 129
Users, importing 53

V

Valid fingerprints 101, 115
Variables 117, 121, 122, 144, 146, 148, 153, 155
Virus cleaning 96
Virus scanners
- Configuring 75
- Installing and configuring 54
- Results 96
- Rule condition 96

Virus scanning 70
Viruses 75

W

Wildcards 220
Windows event logs
- Filters 176

Copyright © 2026 Trustwave Holdings, Inc.

About LevelBlue

LevelBlue reduces risk and builds lasting resilience so organizations can innovate and advance their mission with confidence. As the world's most analyst-recognized and largest pure-play managed security services provider, LevelBlue elevates client outcomes that matter: stronger defense, faster response, and sustained business continuity. LevelBlue combines AI-powered security operations, advanced threat intelligence, and elite human expertise to provide the most comprehensive portfolio of strategic advisory, managed security, offensive security, and incident response services.