



Suggested Encryption Policy Guide for MailMarshal SendSecure

INTRODUCTION

MailMarshal SendSecure is a hosted email security service that hosts sensitive email messages from your company on a secure Web portal, allowing message recipients to receive their messages securely using only a Web browser and their Internet connection.

The MailMarshal SendSecure service is configured to accept messages originating from your MailMarshal SMTP gateway and it will automatically encrypt any message you choose to send to it.

MailMarshal SMTP's powerful lexical analysis abilities and content filtering features are used to route messages that contain sensitive content to the SendSecure service. There are many possible ways to implement your chosen encryption policies using MailMarshal SMTP, but this paper will present a few of the more common rule types to give you some ideas.

ROUTING SECURE MESSAGES

Outgoing messages that are deemed to contain sensitive content by MailMarshal SMTP's rules will be routed to the MailMarshal SendSecure service via MailMarshal SMTP's 'route to host' rule action. The host that messages should be routed to is `outbound.sendsecure.marshall8e6.com`.

ENCRYPTION POLICY EXAMPLES

The following examples can be used as guidelines to help you create your own custom email encryption policy.

Encryption by Recipient Group Membership

If your company routinely sends sensitive content to certain known parties, you can choose to create rules that ensure that all messages sent to these parties are securely delivered. For example, the following rule encrypts any message to the 'Manufacturing Suppliers' group.

Standard Rule: Encrypt Messages to Suppliers

- When a message arrives
- Where message is outgoing
- Where addressed to 'Manufacturing Suppliers'
- Set message routing to `outbound.sendsecure.m86security.com`
- And pass message to the next rule for processing

Encryption by Sender Group Membership

If only certain employees within your company need to send confidential content, then you can choose to send only their messages through the SendSecure service. For example, the following rule only encrypts messages sent from the 'Accounting' group to the 'Manufacturing Suppliers' group.

Standard Rule: Encrypt Messages from Finance to Suppliers

- When a message arrives
- Where message is outgoing
- Where addressed both to 'Manufacturing Suppliers' and from 'Accounting'
- Set message routing to `outbound.sendsecure.m86security.com`
- And pass message to the next rule for processing

Encryption by Subject Line Content

If employees want to indicate to MailMarshal that they would like the email to be encrypted, regardless of who it is being sent from, you can create a rule that looks for a special tag in the email messages subject line. For example, an employee sending confidential contracts can ensure that the message is sent via SendSecure by adding '[Secure]' to the email's subject. The following rule examines the messages' header, looking for that pattern.

Standard Rule: Encrypt Messages with [Secure] in the Subject

- When a message arrives
- Where message is outgoing
- Where message contains one or more headers
- '[Secure]'
- Set message routing to `outbound.sendsecure.m86security.com`
- And pass message to the next rule for processing

The message header match details are below:

| | |
|---------------------------|-------------|
| Name | [Secure] |
| Fields to Match Against | Subject |
| Field Parsing Method | Entire Line |
| Match Case | No |
| Optional Exclusion Filter | No |
| Search Expression | \[Secure\] |

Encryption by Message Content

Finally, the message content itself can be used as criteria to determine whether or not a message should be encrypted. MailMarshal SMTP can detect sensitive content using many methods, some examples of which are below. The first example looks for credit card numbers in the content of the message, and routes it to SendSecure accordingly, if found. It uses the CreditCard category script that's included with the default MailMarshal SMTP installation.

Standard Rule: Encrypt Messages with Credit Card Numbers

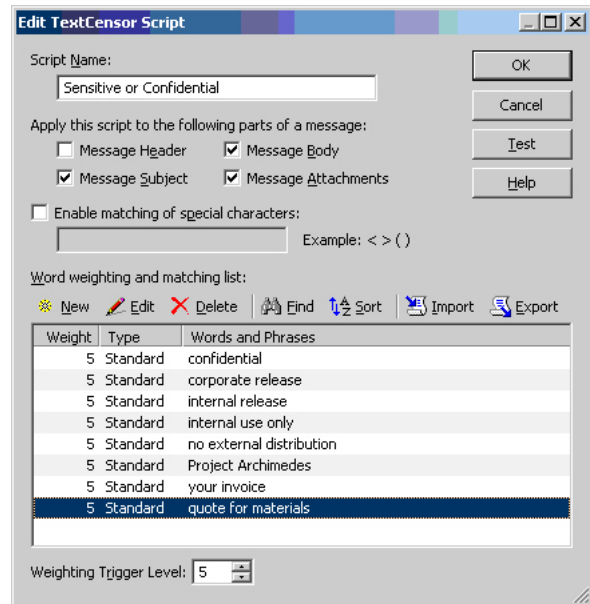
- When a message arrives
- Where message is outgoing
- Where message is categorized as 'CreditCard'
- Set message routing to outbound.sendsecure.m86security.com
- And pass message to the next rule for processing

You can also use custom TextCensor scripts to scan the message for sensitive content. The rule below uses a slightly customized version of the default 'Sensitive or Confidential' TextCensor script shipped with MailMarshal SMTP.

Standard Rule: Encrypt Messages with Sensitive Information

- When a message arrives
- Where message is outgoing
- Where message triggers text censor script(s) 'Sensitive or Confidential'
- Set message routing to outbound.sendsecure.m86security.com
- And pass message to the next rule for processing

A screenshot of the customized TextCensor script is reproduced below.



CONCLUSION

By using MailMarshal SMTP's deep content filtering capabilities, performing automatic encryption of sensitive emails is as simple as creating a few rules. All of the sample policies mentioned above can be used by themselves, in conjunction with one another, or even within a single rule.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Eilerslie, Auckland, 1051
New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 11.10.09