TECHNICAL REFERENCE

MailMarshal (SEG) Cloud Secure Email Encryption Setup

Table of Contents

About This Document

This document provides information for customers who have purchased the Trustwave Secure Email Encryption feature of the MailMarshal/SEG Cloud service.

The steps required are:

1. Confirm that the service is provisioned.
2. Edit the package rules that encrypt the messages by sender or keywords. Set up user matching to control what messages are encrypted.
3. Enable the desired rules.

Note: This document has been updated to reflect the Secure Email Encryption rule package that is provisioned for most customers. Some customers are still provisioned with a legacy package that includes slightly different rules.

1 Provisioning and Configuration

Before you set up and enable rules, ensure that the Secure Email Encryption service has been provisioned for your organization.

Trustwave or your reseller will:

- Contact you to gather required information
- Inform you that the service has been provisioned and is ready for configuration

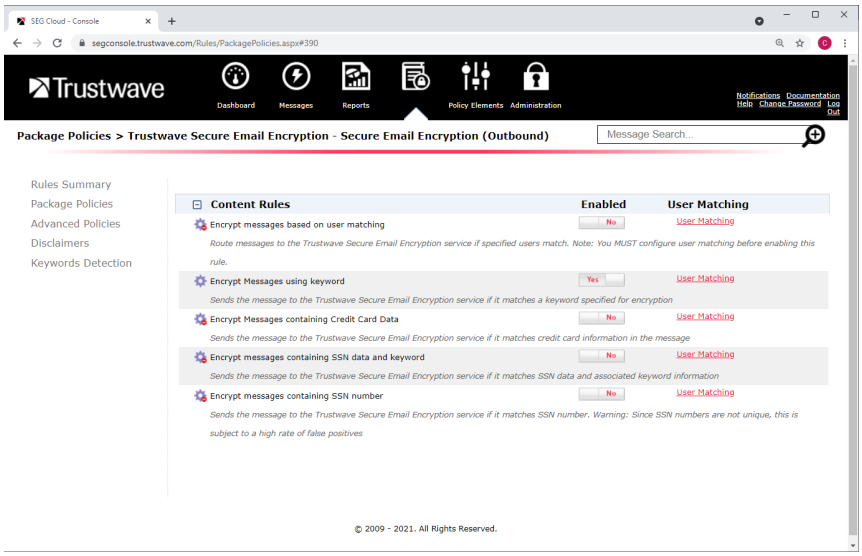
2 Editing Rules

To set up the service, configure user matching (if required) for each rule.

Tip: Most customers have a policy that encrypts messages based on a combination of sender (email address) and keywords or sensitive data. Messages from other senders are not encrypted, and messages that do not contain the keywords or sensitive data are not encrypted.

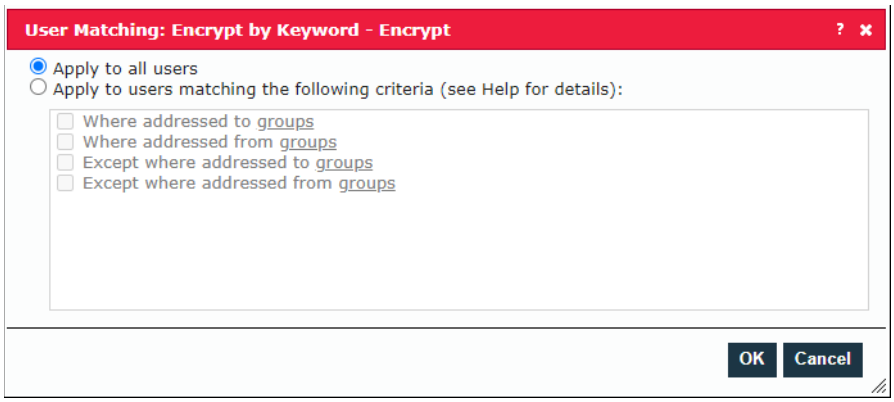
4. In the SEG Cloud Console, navigate to **Rules > Package Policies**.
5. Under Encryption, click **Secure Email Encryption (Outbound)** to see the list of rules.

Tip: See Section 4 of this document for a full definition of each rule.



6. For each rule you want to enable, click **User Matching**. Select the matching criteria and enter user group information to control what messages are encrypted, and then click **OK**.

Note: To create and manage Groups for User Matching, see **Policy Elements > Groups**.



7. Repeat for each rule that you want to enable.

3 Enabling the Service

To enable the service, once all new rules are correctly configured:

1. On the Package Policies page, enable Secure Email Encryption (Outbound) by clicking the slider.

2. Click the policy name **Secure Email Encryption (Outbound**) to view the rules.
3. For each rule that you have configured and want to enable, click the slider to enable the rule.
4. Once the rules have been applied on the processing servers (approximately 15 minutes), you can test encryption by sending messages to trigger each rule.

4 List of Encryption Rules

The Secure Email Encryption (Outbound) package includes the following rules:

Rule: Encrypt messages based on user matching

User Matching Allowed

Route messages to the Trustwave Secure Email Encryption service if specified users match. Note: You MUST configure user matching before enabling this rule.

When a message arrives
And the message is outgoing
Then
Write log message with 'Encrypted Message - by Recipient'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages using keyword

User Matching Allowed

Sends the message to the Trustwave Secure Email Encryption service if it matches a keyword specified for encryption.

Note: This rule triggers if any of the following words are found in the message subject (not case sensitive): encrypt, safe, secure, secured.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – Keyword in subject line'
Then
Write log message with 'Encrypted Message - Keyword'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages containing Credit Card Data

User Matching Allowed

Sends the message to Trustwave Secure Email Encryption service if credit card information is found in the message.

Note: This rule triggers if both the “categorized” and TextCensor conditions trigger.

The “categorized” component checks for well-formed credit card numbers in the subject, body, and top level attachments of a message, using a proprietary method.

The TextCensor component searches the subject, body, and attachments (not case sensitive).

- It triggers immediately if one of the following words or phrases is found: JCB, American Express, Amex, credit card, Diners Club, DiscoverCard, Mastercard, Visa
- It triggers if more than one of the following words is found: card, credit, Diners, Discover, number, No., Num

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Keyword list – Credit Card'
And where messages is categorized as 'CreditCard'
Then
Write log message with 'Encrypted Message – Credit Card Number'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages containing SSN data and keyword

User Matching Allowed

Sends the message to Trustwave Secure Email Encryption service if it matches SSN data and associated keyword information.

Note: This rule triggers if both the "categorized" and TextCensor conditions trigger.

The "categorized" component checks for well-formed US Social Security numbers in the subject, body, and top level attachments of a message, using a proprietary method.

The TextCensor component searches the subject, body, and attachments (not case sensitive).

- It triggers immediately if one of the following words or phrases is found: SSN, Social Security
- It triggers if more than one of the following words is found: Security, Social, number, No., Num

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Keyword list – Social Security'
  And where messages is categorized as 'SocialSecurity'
Then
Write log message with 'Encrypted Message – Social Security Number'
  And rewrite message headers using 'Add encryption routing header'
  And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages containing SSN data

User Matching Allowed

Sends the message to Trustwave Secure Email Encryption if it matches a SSN number. Warning: Since SSN numbers are not unique, this is subject to a high rate of false positives.

Note: This rule triggers on the presence of strings that look like US Social Security Numbers, in the message subject or body.

This rule is subject to false positives (excessive triggering) because Social Security Numbers are not uniquely distinguishable from other groups of nine digits such as telephone numbers.

The TextCensor component searches the subject, body, and attachments (not case sensitive).

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – Social Security Number Anywhere'
Then
Write log message with 'Encrypted Message – Social Security Number'
  And rewrite message headers using 'Add encryption routing header'
  And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.