



CUSTOMER GUIDE

Trustwave MailMarshal Cloud

September 2023

Legal Notice

Copyright © 2023 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

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




support.trustwave.com/MailMarshalCloud/

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Formatting Conventions

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

Format and Symbols	Meaning
<u>Crimson Underline</u>	A crimson 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.

Definitions

This manual uses the following naming conventions.

Term	Definition
Service Provider	Trustwave or the Reseller for a Customer.
Reseller	An organization that markets and manages hosted services to customers.
Reseller User	The personnel who manage application configuration and settings for customers of the Reseller.
Customer	An organization that subscribes to the hosted service.
Customer Administrator	The personnel who manage local configuration and email content security settings for the Customer organization.
User	Any individual email user within the Customer organization.

Table of Contents

- Legal Notice ii**
- Formatting Conventions iii**
- Definitions iv**
- 1 Introduction 7**
 - 1.1 What Is Trustwave MailMarshal (SEG) Cloud? 7
- 2 Understanding MailMarshal Cloud Administration 8**
 - 2.1 Dealing with False Positives 8
 - 2.2 Understanding the Customer Interface 8
 - 2.2.1 Logging in to the Customer Console 8
 - 2.2.2 Customer Interface Features 9
 - 2.3 Understanding Wildcard Characters 10
- 3 Using the Customer Interface for Monitoring, Auditing, and Reporting 11**
 - 3.1 Reports 12
 - 3.1.1 Reports on Demand 12
 - 3.1.2 Scheduled Reports 12
 - 3.2 Report Descriptions 13
 - 3.2.1 Messages 13
 - 3.2.2 Summary 14
 - 3.3 Notifications 16
 - 3.4 Message History 16
 - 3.4.1 Working with Message History results: 17
 - 3.5 Rejected Messages 18
 - 3.6 Message Queues 18
 - 3.7 Audit History 19
- 4 Using the Customer Interface for Policy Configuration 20**
 - 4.1 System Configuration 21
 - 4.1.1 General Configuration 21
 - 4.1.2 Domains 21
 - 4.1.3 Relays 21
 - 4.1.4 Azure Information Protection 22
 - 4.1.5 Syslog 22
 - 4.2 Security Configuration 22
 - 4.2.1 System Logins 22
 - 4.2.2 IP Access 23
 - 4.2.3 Single Sign On 24
 - 4.3 Email Policy 24

4.3.1 Rules Summary	24
4.3.2 Package Policies	25
4.3.3 Disclaimers	25
4.3.4 Keywords Detection	26
4.4 User Groups	26
4.4.1 Creating and Maintaining User Groups	27
4.4.2 Populating a Group	27
4.5 IP Groups	28
4.5.1 Creating and Maintaining IP Groups	28
4.5.2 Populating a Group	28
4.6 Message Digests	29
4.7 Message Templates	30
4.8 Blended Threats Exclusions	31
4.9 Executive Names List	31
4.10 TextCensor Scripts (Keywords Detection)	32
4.10.1 TextCensor Elements	32
4.10.1.1 Wildcards	32
4.10.1.2 Positional Operators	33
4.10.1.3 Logical (Boolean) and Special Operators	34
4.10.2 TextCensor Concepts	34
4.10.2.1 Words	34
4.10.2.2 Phrases	35
4.10.2.3 Symbols and Punctuation	35
4.10.2.4 Word Breaks	35
4.10.2.5 Accented Letters	35
4.10.2.6 Escape Characters	35
4.10.2.7 Case Sensitivity	36
4.10.2.8 Classes	36
4.10.2.9 Named Statements	36
4.10.2.10 Scoring a TextCensor Script	37
4.11 SQM Configuration	37
4.11.1 Configuring SQM	38
4.11.2 Configuring Single Sign On for SQM	38
5 Using the Connector Agent	40
5.1 Getting Started with the Connector Agent	40
5.2 Changing the Connector Agent Settings	42
5.3 Monitoring Connector Agent Activity	42

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

1.1 What Is Trustwave MailMarshal (SEG) Cloud?

Trustwave MailMarshal (SEG) Cloud is an email content security application for organizations, hosted by Trustwave. Through MailMarshal Cloud, the complexity and cost of email content security for the user organization can be notably reduced.

The Customer Interface allows customer administrators to adjust settings and review email activity. Depending on the settings configured, customer organizations can filter messages based on their own requirements.

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



Note: For definitions of the terms used in this document to describe organizations and MailMarshal Cloud components, see "Definitions" on page iv.

2 Understanding MailMarshal Cloud Administration

MailMarshal Cloud provides a website interface for customer administration and end-user quarantine management of the system.

The Customer Console allows Customer Administrators (as well as Resellers) to configure and monitor settings.

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



Note: Policy configuration changes that you make in the Console are applied four times each hour. When you make a change it could take up to 20 minutes to become effective. User group and IP group member updates are normally effective within two minutes.

MailMarshal Cloud also provides a Spam Quarantine Management website that allows end users to manage quarantined items. For setup details, see “SQM Configuration” on page 37.

You can also set up a Spam Reporter plug-in for Outlook (available in Outlook 365). For details, see MailMarshal Cloud Knowledgebase article [Q21067](#).

2.1 Dealing with False Positives

MailMarshal Cloud has an industry leading level of accuracy in classifying spam and valid email. However, you may find that legitimate messages have been quarantined as spam (false positive), or spam messages have been delivered to users.

MailMarshal Cloud allows you to report and deal with these messages quickly and efficiently. For detailed guidance, see MailMarshal Cloud Knowledgebase article [Q21199](#). Setup of some related features such as Digests and SQM is covered in this Guide.

2.2 Understanding the Customer Interface

MailMarshal Cloud provides a website interface for customers to configure, monitor, and report on email content security.

To access the Console navigate to `https://console.region.mailmarshal.cloud` where *region* is your service region: US, AU, or EU.

2.2.1 Logging in to the Customer Console

To log in to the MailMarshal Cloud Customer Interface, use a current supported version of a major Web browser:

- Basic testing was performed with Edge, Firefox, Chrome, and Safari.
- JavaScript and cookies must be allowed.



Note: You can connect using other browsers, but only the browsers named above were tested.

Access to the Customer Interface could be limited to certain IP address ranges. For information about allowed ranges or to request changes, contact Trustwave or your Reseller.

On the welcome screen, enter a login name (`user@domain`) and password as supplied to you.

If you enter incorrect credentials too many times, your account will be locked out temporarily. To unlock an account immediately, contact a user with full privilege on the Management Interface, or Trustwave.

Once you are logged in, the main window displays your login at the top left of the window.

2.2.2 Customer Interface Features

The Customer Interface features a main menu at the left, grouped by functional areas. Selecting an item usually opens a sub-menu with additional options, and a content page at the right (the first available content page from the sub-menu).

In the Mobile view of the Console, you can access the main menu using the chevron at top right, and the sub-menu using the “hamburger” icon below the chevron.

- Most pages include a Help link at the top right, or in the toolbar above a list. Help provides detailed information about the page purpose and the fields.
- Many fields and controls include an Info tool tip that provides basic information.
- Content pages often show a list of items and a number of action buttons.



Note: In the Mobile view or on browser windows less than 1800 pixels in width, some list columns are not shown.

- You can usually sort the list by clicking column headers.
- You can filter on text in the list using the Filter For field. This feature does not filter on dates or numbers.
- You can make changes to an item by selecting it and using the action buttons above the list, or by right-clicking to open a context menu.
- You can add a new item using the Add button above a list.
- For message history, you can take action on multiple items using CTRL-click or shift-click to select, and using the action buttons at the top of the list.

Where a feature has a range of options or complex configuration, clicking a link displays the options on a child pane or pop-up. Enter or select options and then click **Save** to return to the parent window. Child panes and pop-ups include detailed Help for the fields and options.

2.3 Understanding Wildcard Characters

You can use wildcard characters in Message History searches (see “Message History” on page 16) and User Group entries (see “IP Groups” on page 28). MailMarshal Cloud supports this syntax:

Table 1: Wildcard Characters

Character	Function
*	Matches any number of characters
?	Matches any single character
[abc]	Matches a single character from a b c
[!abc] or [^abc]	Matches a single character except a b or c
[a!b^c]	Matches a single character from a b c ! ^
[a-d]	Matches a single character in the range from a to d inclusive
[^a-z]	Matches a single character not in the range a to z inclusive

The table below gives some examples of results of the wildcard syntax.

Table 2: Wildcard Examples

Pattern	Matches
*.ourcompany.com	pop.ourcompany.com hq.ourcompany.com
mail[0-9].ourcompany.com	mail5.ourcompany.com <i>but not</i> maila.ourcompany.com
mail[!0-9].ourcompany.com	mails.ourcompany.com <i>but not</i> mail3.ourcompany.com



Note: The !, -, and ^ are special characters only if they are inside [] brackets. To be a negation operator, ! or ^ must be the first character within [].

3 Using the Customer Interface for Monitoring, Auditing, and Reporting

The MailMarshal Cloud Customer Interface provides a number of views to assist in daily administration of email flow and server health. These include:

Overview

- **Dashboard:** Shows a graphical summary of message processing and classifications for the current day, as well as information about queued messages and product features.
- **Reports:** Allows you to generate summary and detail reports about email flow, threats, and billing information. Reports can be viewed on the Customer Interface, or scheduled and sent by email. See “Reports” on page 12.

Management

Allows you to perform daily email management and review changes. This section also includes policy setup items which are covered in detail in the chapter “Using the Customer Interface for Policy Configuration” on page 20.

- **Messages**
 - **Message History:** Allows you to perform a search for messages or history records in the message database. See “Message History” on page 16.
 - **Rejected Messages:** Allows you to perform a search for messages rejected by a Connection rule or policy. See “Rejected Messages” on page 18.
 - **Message Queues:** Shows the status of incoming and outgoing messages for each server and for each destination route (email domain or forwarding server). See “Message Queues” on page 18.
- **Email Policy:** Allows you to view a list of configured email rules, and manage package policies. See “Email Policy” on page 24.
- **Policy Elements:** Allows you to manage items used in rules. See detailed sections in “Using the Customer Interface for Policy Configuration” on page 20.
- **SQM Configuration:** Manage the web-based end user management module of MailMarshal Cloud. See “SQM Configuration” on page 37.
- **Audit History:** Review Customer Interface activity, and changes to MailMarshal Cloud configuration, for any period. See “Audit History” on page 19.
- **Connector Agent History:** Review MailMarshal Cloud Connector Agent activity, and changes to Connector Agent configuration. This item is present if Connector Agent is enabled. See “Monitoring Connector Agent Activity” on page 42.
- **Notifications:** Provides the latest news and updates about the MailMarshal Cloud system.

Configuration

Allows you to view and configure general features of the MailMarshal Cloud interface and email filtering. See the next chapter for details.

Support

Allows you to access help and documentation.

3.1 Reports

Reports allow you to generate summary and detail reports about email flow, threats, and billing information. Reports can be viewed on the Customer Interface, or scheduled and sent by email.



Note: Reports are based on Message History data. This data is retained for 100 days.

3.1.1 Reports on Demand

Any MailMarshal Cloud report can be run on demand, except as noted in the list below.

To run a report:

1. In the Customer Interface, expand **Reports**.
2. Select **Messages** or **Summary** reports.
3. In the right pane, select a report from the list.
4. If required, enter parameters to limit the report data, and then click **Generate**. Parameters generally include data range and classification or user selection. For details of the available parameters, see Help for the specific report.
5. The report results display in the Customer Interface. You can click column headings to sort the results. You can click + icons to see details of a group or category.
6. You can also enter an email address to deliver a copy by email.

3.1.2 Scheduled Reports

Any MailMarshal Cloud report can be scheduled to run periodically. Scheduled reports are delivered by email to one or more recipients.

The list of scheduled reports includes all reports scheduled by any administrator for your customer organization.

To schedule a report:

1. In the Customer Interface, expand **Reports > Scheduled Reports**.
2. Click **Add**.
3. Select the report type.

4. Enter a name for the report, and select the schedule and recipients.



Tip: You can enter multiple recipient email addresses. Click **+** or press Enter to open a new input row.

5. If required, enter parameters to limit the report data, and then click **Save**. For details of the available parameters, see Help for the specific report.



Note: You cannot specify a reporting period for scheduled reports. The period covered by a scheduled report depends on the schedule. For instance if a report is scheduled daily, each report generated covers the day ending when the report is generated.

6. The scheduled report is listed in the Customer Interface.

To edit or delete a scheduled report:

1. In the Customer Interface, expand **Reports > Scheduled Reports**.
2. To enable or disable scheduled generation of a report, select it and click **Enable** or **Disable**.
3. To edit the schedule or parameters, click **Edit**.
4. To delete the scheduled report instance, click **Delete**.

3.2 Report Descriptions

The following types of reports are available in MailMarshal Cloud.

For details of the report parameters and the fields on each report, see Help for the specific report.

3.2.1 Messages

These reports provide detailed data about the messages passing through MailMarshal Cloud.

Domain Traffic

Traffic volume and total cost for each domain managed.

Formats available: Both

Records Returned: All

Messages by Classification Per User

Number of messages logged for each user in each classification.

Formats available: Text Only

Records Returned: All

Messages by Classification Trend

Number of messages and total size logged per day in each classification.

Formats available: Text Only

Records Returned: All

Messages By Domain

Summary of message traffic inbound and outbound for each domain managed. Optionally includes a summary of messages classified by reason (such as spam, viruses, or encryption requirements).

Formats available: Text and Graphic

Records Returned: All

Messages Detail By Classification

Detail of messages logged with a specific classification. This report can only be run as a scheduled (daily or weekly) report.

Formats available: Text Only

Records Returned: Defined by menu selection

Messages Per Classification Per User

Number of messages logged per user, per classification.

Formats available: Text Only

Records Returned: Defined by menu selection

Most Active Users

Most active users in the system by message size and number of messages.

Formats available: Text Only

Records Returned: Defined by menu selection

Top Sources of Blocked Messages

List of domains sending messages that are quarantined by rules. Useful to determine which senders breach the configured policies the most.

Formats available: Text, and Graphic if the number of records requested is 25 or fewer

Records Returned: Defined by menu selection

3.2.2 Summary

These reports provide an overview of message traffic passing through MailMarshal Cloud.

Bandwidth Summary by Email Address

Utilization and cost data for each email address

Formats available: Text and Graphic

Records Returned: All



Note: If you run this report for a user group that includes other groups, all cost data will be calculated using the settings of the parent group. If you run this report for one or more domains, all cost data will be calculated using the settings of the most costly group for each message.

Estimated Bandwidth Savings

Estimated savings on bandwidth due to MailMarshal Cloud rule actions

Formats available: Text and/or Graphic

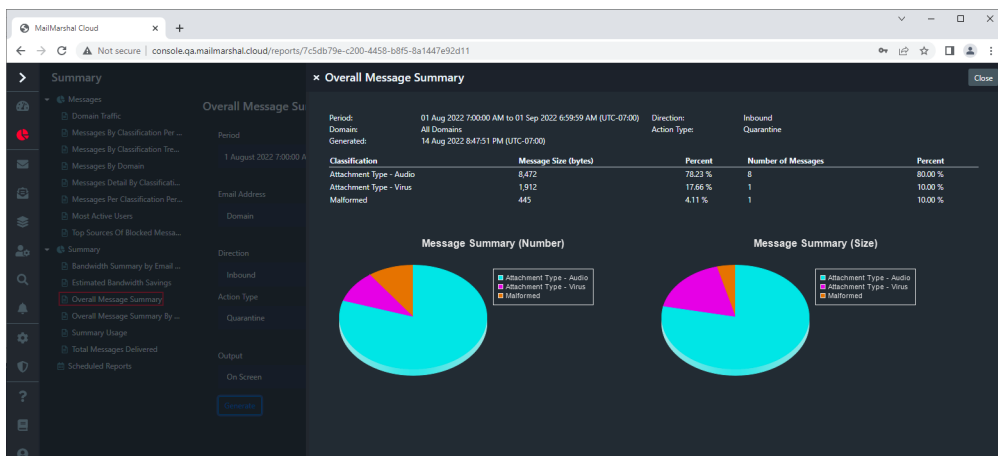
Records Returned: All

Overall Message Summary

Combined summary of all blocked and accepted messages, split into the classifications that have been logged.

Formats available: Text and/or Graphic

Records Returned: All



Overall Message Summary By Domains

Combined summary of all blocked and accepted messages for each local domain, split into the classifications that have been logged.

Formats available: Text Only

Records Returned: All

Summary Usage

Overall view of messages rejected, message volume, bandwidth, and quarantine actions for a selected user group or domain.

Formats available: Text and Graphic

Records Returned: Defined by menu selection

Total Messages Delivered

Statistical summary of message processing during the selected period.

Formats available: Text Only

Records Returned: All

3.3 Notifications

Notifications provide important information about MailMarshal Cloud, including system notices and details of new functionality.

To view Notifications, click the Notifications link at the top right of any page.

When you log on, the Customer Interface shows a list of new and important notifications. You can choose to see only urgent notifications at logon. You can always see all current notifications (including items you have read) on the main Notifications page.

3.4 Message History

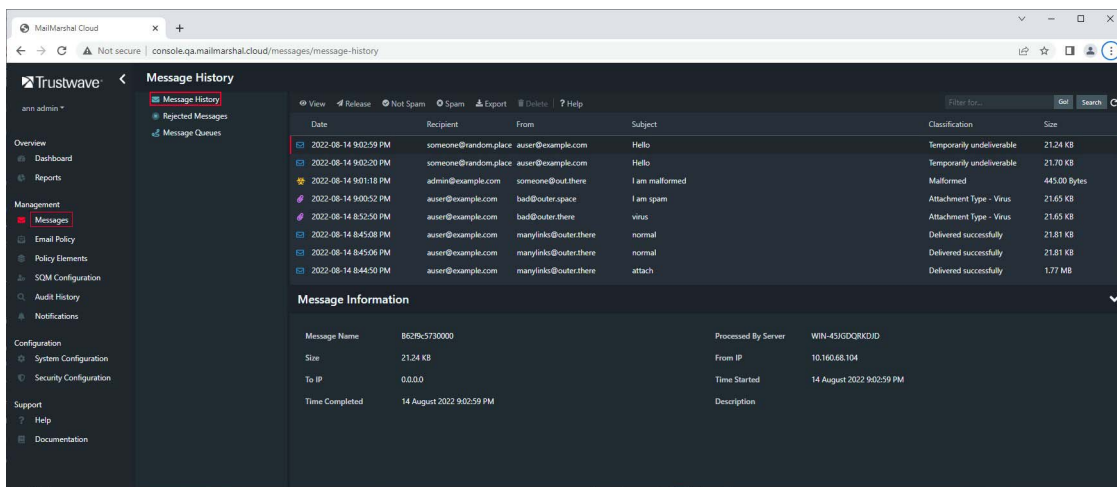
Message History provides a search for messages or history records in the message database. For full details of the options, see Help.



Note: Message History data is retained for 100 days.

To perform a Message History search:

1. On the main menu of the Customer Interface click **Messages > Message History**.
2. Enter or select parameters that define the messages you want to find.
3. Click **Search** to begin searching.



You can search using some or all of the following parameters. For more details, see Help.

- **Date:** Specify a time period or range of dates to search.
- **In:** Specify the field or part of the email message to search.
- **Search For:** Specify the text to search for. Leave blank to find all messages.



Notes:

- You can add more search criteria by clicking the + icon at the right of these fields.
- You can use wildcard characters in the first Search For text field only. For details, see Help.
- **Domains:** If you have more than one email domain, you can select the domain(s) to include in the search. Use shift-click to select more than one domain.
- **Direction:** Specify the message direction (inbound or outbound) or all.
- **Type:** Specify the record type(s) to search.
- **Include Deleted:** Include in the results messages that have already been processed.
- **Classification:** Specify the classification to search.

3.4.1 Working with Message History results:

The results are presented in table form. The available options depend on the type of result (message or history record) and on the permissions for your Customer Interface login.



Note: Scroll down to load more messages in the list.

- Select a single message to see basic processing details and any manual processing actions taken in the **Message Information** section below the list.
- Select a single message and click **View** to see the message content and processing logs (if available). On the message viewer, click **Release** to see options for releasing or forwarding the message.

To take action on one or more messages, select the messages by highlighting, and click **Release** to choose the type of action (**Continue processing, Reprocess, Pass Through, or Forward**). You can also notify the sender of the action, and you may be able to choose whether to delete the message. You may also be able to report the message as Spam or Not Spam (if it has been wrongly classified). You may be able to delete messages without taking any other action.

To filter the list by text (in subject or email addresses), use the **Filter For** field. To search again or limit dates, click the **Search** button.

For more details of the Message Viewer and Process windows, see Help.

3.5 Rejected Messages

The Rejected Messages window provides a search for message rejection actions based on connection rules or system-wide connection policies. These rejections occur while delivery is being attempted, based on limited information.

The results are presented in table form. Results are informational only. It is not possible to release or accept messages from these results.

For full details of the search options and results, see Help

To perform a Rejected Messages search:

1. On the main menu of the Customer Interface click **Messages > Rejected Messages**.
2. Enter or select parameters that define the messages you want to find.
3. Click **Search** to begin searching.

You can search using some or all of the following parameters. For more details, see Help.

- **Date:** Specify a time period or range of dates to search.
- **In:** Specify the recipient or sender field par to search. Only the from and to addresses (or domains) are available in this search.
- **Search For:** Specify the text to search for. Leave blank to find all messages



Notes:

- "All fields" supports entry of a full email address. The other selections expect a user or domain name, not a full email address.
- You can add more search criteria by clicking the + icon at the right of these fields.
- **From IP Start:** Specify the beginning of the source IP range to search.
- **From IP End:** Specify the end of the source IP range to search.
- **Max Rows:** Specify the number of results to return.

3.6 Message Queues

The Message Queue display shows the status of your incoming and outgoing messages. The list shows information for each destination route (email domain or forwarding server) that messages are delivered to.

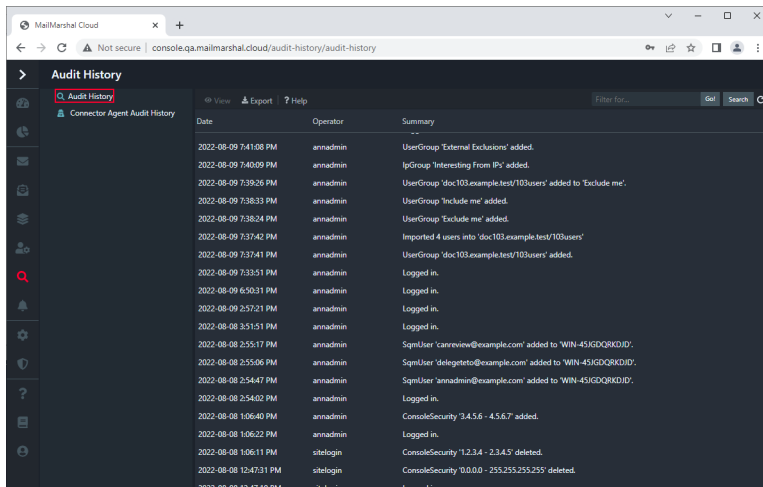
- Select a route and click **View** to see a list of all messages for the route. In the details listing you can take action on individual messages.
- Click **Retry** to request MailMarshal Cloud to retry delivery to the route immediately.
- Click **Delete** to delete all pending messages for the route.

3.7 Audit History

Audit History allows you to review Customer Interface activity, messages released or reprocessed, and changes to MailMarshal Cloud configuration, for any period.

To perform an Audit History search:

1. On the main menu of the Customer Interface, select **Audit History**.
2. In the result page, scroll down to see additional entries.
3. To find specific items, click Search. See Help for details After you generate the Audit History, you can save it to a CSV file. To create the file, click **Export**.



The screenshot shows the MailMarshal Cloud Audit History page. The page title is "Audit History" and it includes a search bar and an "Export" button. The main content is a table with the following columns: Date, Operator, and Summary. The table contains 20 rows of audit events, including actions like adding or deleting UserGroups, logging in, and adding or deleting ConsoleSecurity items.

Date	Operator	Summary
2022-08-09 7:41:08 PM	annadmin	UserGroup 'External Exclusions' added.
2022-08-09 7:40:09 PM	annadmin	IpGroup 'Interesting From IP' added.
2022-08-09 7:39:26 PM	annadmin	UserGroup 'doc103.example.test/103users' added to 'Exclude me'.
2022-08-09 7:38:33 PM	annadmin	UserGroup 'Include me' added.
2022-08-09 7:38:24 PM	annadmin	UserGroup 'Exclude me' added.
2022-08-09 7:37:42 PM	annadmin	Imported 4 users into 'doc103.example.test/103users'
2022-08-09 7:37:41 PM	annadmin	UserGroup 'doc103.example.test/103users' added.
2022-08-09 7:33:51 PM	annadmin	Logged in.
2022-08-09 6:50:31 PM	annadmin	Logged in.
2022-08-09 2:57:21 PM	annadmin	Logged in.
2022-08-08 3:51:51 PM	annadmin	Logged in.
2022-08-08 2:55:17 PM	annadmin	SqmUser 'canreview@example.com' added to 'WIN-45IGDQRKDD'.
2022-08-08 2:55:06 PM	annadmin	SqmUser 'delegateto@example.com' added to 'WIN-45IGDQRKDD'.
2022-08-08 2:54:47 PM	annadmin	SqmUser 'annadmin@example.com' added to 'WIN-45IGDQRKDD'.
2022-08-08 2:54:02 PM	annadmin	Logged in.
2022-08-08 1:06:40 PM	annadmin	ConsoleSecurity '3.4.5.6 - 4.5.6.7' added.
2022-08-08 1:06:22 PM	annadmin	Logged in.
2022-08-08 1:06:11 PM	sitelogin	ConsoleSecurity '1.2.3.4 - 2.3.4.5' detect.
2022-08-08 12:47:31 PM	sitelogin	ConsoleSecurity '0.0.0.0 - 255.255.255.255' deleted.

4 Using the Customer Interface for Policy Configuration

The MailMarshal Cloud Customer Interface provides a number of views that allow you to customize the policies applied to your email, and to give email users the power to manage quarantined messages. The views include:

System Configuration

- **General Configuration:** View and edit contact information for the customer (if permitted).
- **Domains:** Add and edit details of the email domains that MailMarshal Cloud manages for you. If permitted, you can change delivery information for an existing domain. See “Domains” on page 21.
- **Relays:** View and edit information about servers that are allowed to send email “from” your managed domains (known as “relaying”). Permission to make changes is at the service provider’s discretion. See “Relays” on page 21.
- Other items may be present, including Azure Information Protection and Syslog. These items are only available if licensed separately.

Security Configuration

- **Logins:** List and manage Customer Interface logins for your domains. See “System Logins” on page 22.
- **IP Access:** Control the locations from which users in your organization can access the Customer Interface. See “IP Access” on page 23.
- **Single Sign On:** Set up SAML based SSO for the Console and/or SQM.

Email Policy

Allows you to view a summary of the rules that apply to your email, and configure some rules. Available items depend on the licensed features.

- **Rules Summary:** Displays a listing of the policy that actually applies to your email, including comments and complete descriptions of each rule.
- **Customer Packages:** Displays a listing of policies and rules that you can apply to your email. You can customize the policy by enabling or disabling some rules, or by applying rules to specific user groups.

Policy Elements

Allows you to view and configure elements that are used in rules, such as User Groups, IP Groups, message digests, message templates, and filtering functions. Available items depend on the licensed features.

SQM Configuration

Allows you to configure the web-based end user management module of MailMarshal Cloud.



Note: Policy configuration changes are applied four times each hour. When you make a change it could take up to 20 minutes to become effective. User group and IP group member updates are normally effective within two minutes.

4.1 System Configuration

The items in this section allow you to view and configure general features of the MailMarshal Cloud interface and email filtering.

4.1.1 General Configuration

The Configuration page allows you to view (and if permitted, to update) basic contact information, time zone setting (used for digest generation and Customer Interface displays), and email addresses used for notifications.

4.1.2 Domains

The domains list provides information about each of the email domains that MailMarshal Cloud manages for the customer, and lists basic information about each domain.

For details of the columns and available actions, see Help.

You can filter the list using the field at the top.

To add a new domain, click **Add**. To edit an existing domain, highlight it and then click **Edit**. Many settings are available only when editing.



Note: When you add a domain, you must also add a special value to the DNS entries for the domain. MailMarshal Cloud will verify your ownership of the domain by checking this value before activating the domain. For full details see Help..

For each domain, you can configure DKIM signing and DMARC processing. You can set custom email addresses for notifications from the domain. You can edit the Executive Names List for this domain. You can change the Cost values (used in reporting only). If permitted, you can change delivery settings for the domain.

4.1.3 Relays

The Relays page allows you to view (and if permitted, to update) information about servers that are allowed to send email “from” your managed domains (known as “relaying”).

Permission to make changes to these lists is at Trustwave’s discretion.

The page includes two lists:

Relay Entries

A list of individual servers or IP ranges allowed to relay. Servers that are used to deliver mail to your domains are always permitted to relay. To add an entry to this list, click **New**. To edit or delete an entry, use the icons to the right of each line.



Note: If you add or edit an entry that would duplicate or overlap an available Relay Group, you will be notified and you might not be able to save the entry. See Help for details.

Relay Groups

A list of pre-configured sets of relay servers, maintained by Trustwave. To enable or disable use of any group, use the toggle to the right of each line.

4.1.4 Azure Information Protection

This page allows you to enter details required to use Azure Information Protection and enable the functionality (to decrypt and inspect traffic passing through the gateway). Availability of this item is at the discretion of the Service Provider.

4.1.5 Syslog

The Syslog section allows you to configure server settings and record templates to deliver email processing information to a Syslog server. Access to Syslog and degree of configurability are at the discretion of the Service Provider. For details of the options, see Help.

4.2 Security Configuration

The items in this section allow you to control access to the web interface for your organization.

4.2.1 System Logins

The Logins listing allows you to view and manage all user names allowed to access MailMarshal Cloud for the customer.

You can control each login's access to various functions of the MailMarshal Cloud Customer Interface

To work with logins, on the main menu of the Customer Interface select **System Configuration > System Logins**.

The default view shows the following columns:

- **Full Name:** The personal name of the user.
- **User Name:** the login name for the user.



Notes:

- Users log in with `User Name@<the customer's domain>`
- If Single Sign On is configured, this must be a valid user name for the Identity Provider.

- **Password or Auto Generate Password:** If Auto Generate is selected, a secure password is created and the user must reset the password before logging in. You can also choose to create a password manually.
- **Read Only:** Indicates whether the login has permission to make changes to settings.
- **Status:** Indicates whether the login is temporarily locked because of too many invalid logon attempts.
 - **Disabled:** Shown by red X on the user icon. Indicates whether the login can be used.
 - **Primary:** Shown by crown on the user icon. Indicates that the login is the primary login for the customer. Primary logins are automatically granted access to new elements such as groups and classifications. For details, see Help.



Note: The Primary login cannot be deleted. However, the Primary login user or a Site Login user can assign another login as Primary.

Logins can be marked as deleted. To show deleted logins in the list, select **Show Deleted**.

To add a login, click **Add**. For details of the fields and options, see Help.



Note: The login names `Sitelogin` and `Supportlogin` are reserved. You cannot create logins with these names. Also, if any other administrative login has permission to view or edit the configuration for your customer company you cannot create a login with that name in the Customer Interface.

To edit an existing login, click the name or click **Edit** . You can set access options including:

- Types of message and history records that can be searched, delete on release, and read-only access, and the ability to report messages as Spam or Not Spam, using the **General** tab.
- Policy elements and rules, and email queues, using the **Roles** tab.
- Email processing functions (depending on the message classification) using the **Mail Security** tab.
- Email processing functions (depending on the message sender or recipient) using the **Groups** tab.

For details of the fields and options, see Help.



Note: Some functionality mentioned in Help is not currently enabled in the MailMarshal Cloud environment.

To unlock a login, select it and then click **Unlock**.

To delete a login, select it and then click **Delete**.

To enable or disable an existing login, right-click and select the appropriate option.

4.2.2 IP Access

The IP Access list allows you to control the network locations from which users in your organization can access the Customer Interface.

- By default access is permitted from all locations.
- To restrict access, add one or more permitted or denied ranges.

- To make exceptions within a permitted or denied range, move the ranges up or down. Effective access is determined by the first entry that matches the connecting IP, in top down order.



Note: Use caution when restricting access or deleting items from this list. If you remove your access, you will not be able to log on. The Service Provider can restore access if necessary.

4.2.3 Single Sign On

The Single Sign On pages allow you to configure SAML SSO Identity Providers that will be used to control access to the Customer Interface and/or SQM. From these pages you can add the required information, and get the metadata you need to set up the link at the provider side. This option is available if configured for your organization.

It is possible to use the same provider for SQM and the Customer Interface, assuming that the entity ID and ACS settings for both are added to the provider. To grant access to the Customer Interface, you must still create user logins and set detailed permissions. Self-registration is not permitted for the Customer Interface, and only logins that are explicitly created will have access. (For more details of SQM SSO, see “Configuring Single Sign On for SQM” on page 38).

To configure Single Sign On (SSO) for the Console:

1. Ask Trustwave (or your Reseller) to enable SSO for your account.
2. Set up a SAML Identity Provider (for example, Microsoft ADFS or Google). Trustwave provides detailed configuration guide documents providing step-by-step instructions for Azure AD, Google G Suite, and Microsoft ADFS (premises). For detailed information, see Help and also see MailMarshal Cloud Knowledgebase article [Q21192](#).
3. In the Customer Interface expand **Security Configuration > Single Sign On > Console Identity Provider**.
4. To add a provider, click **Add**. For details of the fields, see Help.

To download an XML file containing the metadata definitions, click **Provider Metadata**. This file can be imported to the provider (in some cases).



Caution: Ensure that settings are properly configured before enabling SSO. If it is enabled with incorrect settings, no users will be able to log in. To recover from incorrect settings on the Console Identity Provider, you must contact Trustwave or your reseller to adjust settings or disable SSO. In particular note that Azure AD authentication fails if you select the “send requested user name” parameter.

4.3 Email Policy

The Rules section of the Customer Interface allows you to review and customize the policy that is applied to your email.

4.3.1 Rules Summary

To generate a summary of rules that apply to your email, on the main menu of the Customer Interface select **Email Policy > Rules Summary**. The listing can take a few minutes to generate.

For each rule, the listing shows the rule name, a verbose description, and a detailed listing of conditions and actions. These rules are listed within the following types of policies:

- **Enforced Policies:** These policies contain rules configured by Trustwave that are always applied to all messages.
- **Package Policies:** These policies contain rules configured by Trustwave. In some cases you may be able to disable these rules, or apply them to a limited set of users.



Note: The listing only shows rules that are enabled and actually used in email processing. Rules will be applied in the order shown (from top to bottom of the listing). Rules that are available, but disabled, do not display in this listing. To see a list that allows you to make changes, view the Customer Packages.

MailMarshal Cloud can also be configured to allow rule creation by customers (Advanced Policies). If any Advanced Policies are configured they will display in this listing. Advanced Policy usage is not covered in this document.

4.3.2 Package Policies

Package policies are groups of rules that are pre-configured by Trustwave to perform common tasks. Depending on the setup of the packages and rules, you may be able to enable or disable packages or individual rules. You may also be able to apply policies or rules to a limited set of users.



Note: Enabled policies will be applied in the order shown (from top to bottom of the listing). Within each Policy, enabled rules will be applied in the order shown.

To work with policies:

1. On the main menu, select **Email Policy > Package Policies**. Expand the listing to see the available packages and the policies.
2. To enable or disable an existing policy, select it and click the toggle in the **Enabled** column. If this control is not usable, you cannot disable the selected policy.
3. To choose the users (senders and recipients) that this policy will apply to, select it, click **User Matching** and then select groups and actions. If this text is not visible, you cannot set up user matching for the selected policy.

To work with individual rules:

1. From the Package Policy listing, click a policy name to view the list of rules included in the policy.
2. To enable or disable a specific rule, select it and click the toggle in the **Enabled** column. If this control is not usable, you cannot disable the selected policy.
3. To choose the users (senders and recipients) that this rule will apply to, click **User Matching** and then select groups and actions. If this text is not visible, you cannot set up user matching for the selected rule.

4.3.3 Disclaimers

Disclaimers are optional text added to the top or bottom of all messages.

You can choose to enable different disclaimers for inbound and outbound messages.

To work with disclaimers:

1. On the main menu, select **Policy Elements > Disclaimers**. The main pane shows the two available disclaimers.

2. To customize a disclaimer, double-click the name link. Edit the text, and choose whether it should appear at the top or the bottom of messages. You can edit plain text and HTML formatted text separately. See Help for details. Click **Save** to save changes.
3. To enable or disable a disclaimer, select it or right-click and click **Enable** or **Disable**.

4.3.4 Keywords Detection

The Keywords Detection function allows you to quarantine messages based on a list of keywords or phrases that you maintain.

To work with keyword detection:

1. On the main menu, select **Policy Elements > Keywords Detection**. The main pane shows the two available detection items (inbound and outbound).
2. To customize a list of keywords and phrases, select an item and then click **Edit**.
3. By default this feature checks text in the message body. You can choose the parts you want to check.
4. To begin adding keywords, click **Add**.



Note: The keyword detection function (TextCensor Scripts) is powerful and offers many options. For basic details of the available options, see **Help** for each window. For full information about syntax and options, see “TextCensor Scripts (Keywords Detection)” on page 32.

5. When you have finished entering or editing items, click **Save** to save changes. You can also click **Cancel** to exit without saving changes.
6. To enable or disable keywords detection for the inbound or outbound direction, select or right-click the item and click **Enable** or **Disable**.

4.4 User Groups

User groups allow you to apply policy to specific users. MailMarshal Cloud uses SMTP email addresses to perform user matching.

Each MailMarshal Cloud user group is either *Internal* (contains addresses within your email domains) or *External* (contains addresses outside your email domains).

You can create and populate user groups by entering email addresses manually or importing them from text files. You can use wildcard characters when you define groups (for syntax, see “Understanding Wildcard Characters” on page 10).

You can include a user group within another user group. Internal groups can include other Internal groups, and External groups can contain External groups.

In Reports, when you select a user group, members of any included groups will also be reported on.

You can also synchronize user groups from a LDAP server through the Connector Agent, and then include these groups in Internal groups. MailMarshal Cloud updates the membership of synchronized groups automatically on a schedule. To learn about synchronized groups and the Connector Agent, see “Using the Connector Agent” on page 40.

4.4.1 Creating and Maintaining User Groups

To create and maintain user groups, on the main menu of the Customer Interface select **Policy Elements > User Groups**.

To create a user group:

1. On the main menu of the Customer Interface, select **Policy Elements > User Groups**.
2. In the right pane, click **Add**.
3. Enter a name for the group. Optionally enter a verbose description.
4. Choose whether the group is Internal or External.
5. Optionally enter an incoming and outgoing cost per megabyte.



Tip: These values are used for your reporting only and have no effect on email delivery or service cost.

6. Click **Save**.

To edit a user group:

1. On the main menu of the Customer Interface, select **Policy Elements > User Groups**.
2. In the right pane, choose the group type by clicking a tab (Internal, External, or Connector Agent).
3. Double-click a group name to edit.
4. If this group was created in MailMarshal Cloud, you can change the name and description. You cannot change the name of imported groups.
5. Optionally enter an incoming and outgoing cost per megabyte.
6. Click **Save**.

4.4.2 Populating a Group

Initially, an internal or external user group will be empty of users. You can add addresses or wildcard patterns, and you can insert other groups.

To edit the members of a group:

1. On the main menu of the Customer Interface, select **Policy Elements > User Groups**.
2. Double-click the name of a group to edit the membership.
3. To add an individual address or wildcard pattern, click **Add**. Enter the information, and then click **Save**.
4. To insert another group, click **Insert User Group**. In the new window, select one or more groups from the list and then click **Save**.
5. To delete an address or pattern, or remove an included group, select the item and then click **Delete**.
6. To import or export a text file containing email addresses, while editing the group click **Import** or **Export**. Note that included groups are not exported and cannot be imported. By default, importing users replaces the existing membership of the group. For details, see Help.

4.5 IP Groups

IP groups allow you to apply policy based on the IP address from which MailMarshal Cloud received a message (SMTP connection).

IP Groups can contain individual IPv4 or IPv6 addresses, address ranges, and CIDR blocks.

You can include an IP group within another IP group.

4.5.1 Creating and Maintaining IP Groups

To create and maintain user groups, on the main menu of the Customer Interface select **Policy Elements > IP Groups**.

To create an IP group:

1. On the main menu of the Customer Interface, select **Policy Elements > IP Groups**.
2. Click **Add**.
3. Enter a name for the group. Optionally enter a verbose description.
4. Click **Save**.

To edit an IP group:

1. On the main menu of the Customer Interface, select **Policy Elements > IP Groups**.
2. Double-click a group name to edit.
3. You can change the name and description.
4. Click **Save**.

4.5.2 Populating a Group

Initially, an IP group will have no IP address entries. You can add addresses, CIDR blocks, or ranges, and you can insert other IP groups.

To edit the members of a group:

1. On the main menu of the Customer Interface, select **Policy Elements > IP Groups**.
2. Double-click the name of a group to edit the membership.
3. To add an individual IP address, range, or CIDR block, click **Add**. Enter the information, and then click **Save**.
4. To insert another group, click **Insert IP Group**. In the new window, select a group from the list and then click **Save**.
5. To delete an entry, or remove an included group, select a group from the list and then click **Delete**.
6. To import or export a text file containing IP addresses, while editing the group click **Import** or **Export**. Note that included groups are not exported and cannot be imported. By default, importing IPs replaces the existing membership of the group. For details, see Help.

4.6 Message Digests

MailMarshal Cloud allows you to send email summaries to users, notifying them about quarantined messages. Users can review and release the messages directly from the digest email. A digest only lists messages that have not been included in a previous digest.

You can

- Include information about messages in one or more classifications/folders
- Limit the digested messages by user group
- Set a schedule of times each day when the digest will be generated
- Set the look and feel of the digest email, and set options for end user release, by using a specified email template. Depending on your permissions you may be able to create templates, or you may be able to select from templates provided by Trustwave. To learn more about templates, see “Message Digests” on page 29
- Send digest emails to each user with undigested email that meets the criteria, or send all digest emails to a specified address
- Send digest emails to the local recipient of incoming messages, or to the local sender of outgoing messages

To work with message digests in the Customer Interface, on the main menu select **Policy Elements > Message Digests**.



Tips:

- To learn more about the available options for digests, see Help for this area of the Customer Interface.
- When you create a new digest, not all options are shown. To see advanced options, edit an existing digest.
- To control the options available to end users (such as releasing messages and trusting the sender), use digest template options. See “Message Digests” on page 29.

To create a message digest:

1. On the main menu of the Customer Interface, select **Policy Elements > Message Digests**.
2. Click **Add**.
3. On the Digest window, complete the heading information and the required information on each tab. For more information about the fields and options, click **Help**.
4. To add the digest, click **Save**.

To edit a message digest:

1. Double-click the digest name in the right pane of the Customer Interface to view its properties on a tabbed window
2. On each tab, specify the appropriate values. For more information about the fields and options, click **Help**.
3. Click **Save**.

4.7 Message Templates

MailMarshal Cloud uses digest templates to deliver periodic message digests to users who self-manage quarantined messages. For more information about digests, see “Message Digests” on page 29.

Depending on your permissions, you may be able to create a customized template for your message digests. If you do not see the menu item mentioned, you do not have this permission.

To create a digest template:

1. On the main menu of the Customer Interface, select **Policy Elements > Message Templates**.
2. Click **Add Digest**.
3. Give the template a name.
4. Click **Base On** to select a template to use as the basis for your new template. The Message Digest Template is the recommended basis.
5. You can edit the text of the template. In most cases you do not need to change the variables (text in { } brackets).
6. Click **Save** to add the new template.

The variable `$MessageDigestTableHTML` controls the look and content of the email listing. The following arguments are available to customize the behavior of this variable. All arguments are optional.

Table 3: Digest Template Detail Variables

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 4: Digest Template Options

Option	Results
SHOWRELEASE	Show the message release link for each message (default option).
RELEASETRUST	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. If user management of safe senders is disabled (in the Administrator tab of the SQM site), the sender will not be added to the list. <ul style="list-style-type: none"> • The recipient will be automatically provisioned as a SQM user if necessary (limited to your number of licensed users).
NORELEASE	Do not show the message release links.

Table 4: Digest Template Options

Option	Results
RELEASEURL=url	Specify the URL path to the Release web page used for this digest (see example below). Defaults to the URL of the MailMarshal Cloud Spam Quarantine Management website. This option should not be changed in templates without consulting Trustwave.
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 }
```

For details of other variables available in digest templates, see the **Variables** topic in Help.

4.8 Blended Threats Exclusions

This item allows you to maintain a list of domains that will never be rewritten for Blended Threat scanning. Blended Threat scanning checks for malicious links at the time the link is clicked.

The item is present only if the Blended Threats functionality is licensed.

For detail of the functionality, see Help.



Tip: Minimize use of this feature. Blended Threats can be associated with trusted or well known domains.

4.9 Executive Names List

MailMarshal Cloud includes a filter to identify targeted fraudulent email aimed at executives (“business email compromise fraud”).

This item allows you to maintain a list of names and email addresses of executives (such as CEO or CFO) that might be used as the source of fraudulent requests.

To add information to the list:

1. On the main menu of the Customer Interface, select **Policy Elements > Executive Names List**.
2. Add personal names and email addresses (one name or address per line). See Help for details.



Tip: Ensure that the entries contain only plain text email addresses and names. Do not include special characters like * or <> brackets.

3. If the Connector Agent is enabled, optionally select one Connector Agent group. Personal names and email addresses from this group will be added to the Executive Names List. This feature allows you to maintain the list in your Active Directory or LDAP directory.

You can also add Executive Names for each domain. See **System Configuration > Domains**.

4.10 TextCensor Scripts (Keywords Detection)

TextCensor Scripts check for the presence of text content in an email message. MailMarshal Cloud can check one or more parts of a message, including the message headers, message body, and any attachments that can be lexically scanned.

TextCensor Scripts are used by the Keywords Detection feature. TextCensor Scripts are also available to Advanced customers in rule creation.

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.



Tip: The simplest kind of TextCensor Script includes a few items, where each item is a single word, and the script will trigger if any of the words is found in the message. Keywords Detection allows up to 25 items.

4.10.1 TextCensor Elements

TextCensor scripts contain one or more expressions, each consisting of a word or phrase.

4.10.1.1 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.

Wildcards match only letters and digits, and apostrophes or hyphens that are treated as part of words (see “Word Breaks” on page 35). 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.

4.10.1.2 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 5: TextCensor Positional Operators

Operator and Syntax	Matching Results
<p>FOLLOWEDBY</p> <p>A FOLLOWEDBY[=distance] B</p>	<p>The start of B occurs within <i>distance</i> words from the end of A. Returns a set of positions spanning from the start of A to the end of B.</p> <p>dog FOLLOWEDBY hous* matches Dog in the house</p>
<p>NOT FOLLOWEDBY</p> <p>A NOT FOLLOWEDBY[=distance] B</p>	<p>The start of B does not occur within <i>distance</i> words from the end of A. Returns a set containing the positions in A that are not followed by B.</p> <p>dog NOT FOLLOWEDBY=1 hous* matches Dog in the house</p>
<p>PRECEDEDBY</p> <p>A PRECEDEDBY[=distance] B</p>	<p>The end of B occurs within <i>distance</i> words from the start of A. Returns a set of positions spanning from the start of B to the end of A.</p> <p>dog PRECEDEDBY cat matches Cat chasing dog</p>
<p>NOT PRECEDEDBY</p> <p>A NOT PRECEDEDBY[=distance] B</p>	<p>The end of B does not occur within <i>distance</i> words from the start of A. Returns a set containing the positions in A that are not preceded by B.</p> <p>dog NOT PRECEDEDBY=2 cat matches Cat was not chasing dog</p>
<p>NEAR</p> <p>A NEAR[=distance] B</p>	<p>If A occurs within <i>distance</i> words before B the resulting position spans from the start of A to the end of B. If B occurs within <i>distance</i> words before A the resulting position spans from the start of B to the end of A.</p> <p>dog NEAR cat matches Cat chasing dog and also matches Dog chasing cat</p>

Table 5: TextCensor Positional Operators

Operator and Syntax	Matching Results
NOT NEAR A NOT NEAR[=distance] B	Returns the positions of all instances of A where B is not found within <i>distance</i> 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.

4.10.1.3 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 6: 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.
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 <i>count</i> or more word positions; otherwise the result is false.

4.10.2 TextCensor Concepts

The following concepts clarify how TextCensor expressions are evaluated.

4.10.2.1 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).

4.10.2.2 Phrases

A phrase is made up of a series of words separated by word break characters.

4.10.2.3 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`

4.10.2.4 Word Breaks

The sets of characters that are treated as word and number break characters generally follow Unicode standards.

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`

4.10.2.5 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.

4.10.2.6 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 (“\\”).

4.10.2.7 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.

4.10.2.8 Classes

You can use TextCensor Classes to match specific types of characters inside a word, or special types of words.

Table 7: 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".
[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.

4.10.2.9 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.

4.10.2.10 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.

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 8: 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.

4.11 SQM Configuration

The SQM Configuration section is available if the MailMarshal Cloud Spam Quarantine Management Website is enabled for your customer company. SQM allows users to review and release email that has

been quarantined by MailMarshal Cloud. SQM is typically used to manage suspected spam, but it can be used with any inbound or outbound classification.



Note: You can also set up a Spam Reporter plug-in for Outlook (available in Outlook 365). For details, see MailMarshal Cloud Knowledgebase article [Q21067](#).

This section allows you to set up logins that can use the SQM site, and to select the message classifications that contain messages users will be able to manage through the site. For general setup information, see “Configuring SQM” on page 38.

You can also configure Single Sign On to the SQM site using a SAML Identity Provider. For information about setting up SSO, see “Configuring Single Sign On for SQM” on page 38.

4.11.1 Configuring SQM

- To manage SQM logins, in the Customer Interface expand **SQM Configuration > Logins**. You can import logins in bulk, add, edit, and delete logins. For details of the fields and options, see Help. Also see the Single Sign On option below.



Note: If the provider configured self-provisioning for SQM for your tenancy you do not need to create logins. Users can create logins by following a link on the SQM login page. SSO automatically creates logins.

- You can set one or more users as “Administrators” for SQM. SQM administrators when logged in to SQM, can view and manage email and permissions for all SQM logins, using the SQM “Switch User” feature.
- To manage SQM classifications, in the Customer Interface expand **SQM Configuration > Classifications**. To learn which classifications are used for spam or other content you want users to manage, view the Rule Summary. For details of the fields and options, see Help.



Note: Depending on the options set for rules and classifications, a message released from the SQM website could be processed through remaining rules, or passed through with no further processing.

- To view a record of activity in the SQM, including the user performing the action and the email recipient affected, in the Customer Interface expand **SQM Configuration > SQM Audit History**. For details of the available information, see Help.

4.11.2 Configuring Single Sign On for SQM

To configure Single Sign On (SSO) for the SQM:

1. Ask Trustwave (or your Reseller) to enable SSO for your account.
2. Set up a SAML Identity Provider (for example, Microsoft ADFS or Google). Trustwave provides detailed configuration guide documents providing step-by-step instructions for Azure AD, Google G Suite, and Microsoft ADFS (premises). For detailed information, see Help and also see MailMarshal Cloud Knowledgebase article [Q21040](#).
3. In the Customer Interface expand **Security Configuration > Single Sign On > SQM Identity Provider**.
4. To add a provider, click **Add**. For details of the fields, see Help.

5. To download an XML file containing the metadata definitions for the MailMarshal Cloud SQM site, click **Provider Metadata**. This file can be imported to the provider (in some cases).



Notes:

- When a user is authenticated with SAML SSO for the first time, a SQM user is created if the email address is not associated with an existing user, and the user name/email address is added as the alias managed by this login.
- If the provider delivers additional alias information (multiple email addresses), then the additional aliases are added to the list of aliases managed by the user (unless they are already managed by another user).
- New aliases, if any, are added at each login. Existing aliases that are not listed by the provider are not automatically removed from SQM.

When configuring SSO on the Identity Provider site you might be required to enter the names of attributes. SQM uses the following attributes. All attributes are case INsensitive, and spaces are ignored.

FullName, Name

The personal name or friendly name of the user

User, UserName

The primary email address for the user, and their login username. This value is only used if the username is not provided directly by the IDP.

FirstName, GivenName

Used to create Fullname if Fullname is not present

Surname, LastName

Used to create Fullname if Fullname is not present

Email, EmailAddress, EmailAddresses, Alias, Aliases, Emails

Any and all of these values will be added as alias email addresses. Some providers do not allow these attributes to be mapped.

6. Once the identity provider is set up, enable it for all domains by selecting it and clicking **Set Default**. You can also set up multiple providers for specific domains. To set a provider for an individual domain, see **System Configuration > Domains**.

5 Using the Connector Agent

The Connector Agent is an optional module of MailMarshal Cloud. To provide more flexible and effective email content security services, MailMarshal Cloud can use information about a customer's local user groups and email addresses. This information can be synchronized from the customer network to MailMarshal Cloud over HTTPS using the Connector Agent. Connector Agent obtains user email address information from Active Directory and/or LDAP servers, or from a text file maintained manually.

To use a Connector Agent group for policy User Matching, include it in an Internal user group. You cannot select a Connector Agent group directly in User Matching



Notes:

- The Reseller configures each Customer account to allow use of the Connector Agent, and sets the number of groups the Customer can import.
- By default, once the Connector Agent is installed and configured, it will be upgraded automatically as required. If automatic upgrade is disabled, you could be asked to upgrade manually. When upgrade is required, the Connector Agent interface notifies you.

For detailed information about the windows and functions of the Connector Agent, see Help for each window.

5.1 Getting Started with the Connector Agent

To use the Connector Agent, first install the software. Next create one or more connectors that access directory servers. Finally, select user groups that you want to synchronize to MailMarshal Cloud from each connector.



Note: The Connector Agent must be able to connect to the MailMarshal Cloud server in order to obtain licensing information. Many features of the Connector Agent are disabled when it cannot connect.

To install the Connector Agent:

1. Select a server where the Connector Agent will be installed. To use the Active Directory and/or LDAP features, this server must have access to the appropriate servers. This server must also be able to connect via HTTPS to the MailMarshal Cloud Customer Interface server for your account.
2. Log on to the selected server. From the selected server, log in to the Customer Interface. Download the Connector Agent using the link on the Dashboard page.
3. Run the Connector Agent installer.
4. After the installation wizard is complete, run the Configuration Wizard. Be sure to run this wizard as administrator.



Tip: This wizard starts by default during installation. You can also start the wizard later, if required by running the SPE Connector Agent from the Windows Start menu.

Always run the Agent interface as administrator to ensure access to required resources.

5. On the Internet Access page, enter Internet connection and proxy details as required.
6. On the Service Provider Host page

- Enter the **Server URL** for the regional instance where the customer is provisioned. Use the Customer Interface URL.
 - Enter a **Login Name** (user@domain) and **Password** with full permission on the Customer Interface for this customer. Click **Test** to check the connection.
7. On the Connector Agent Upgrade Settings page, choose whether to allow the software to be upgraded automatically over the Web connection as required. If you do not allow automatic upgrades, you will need to upgrade the software manually as required.
 8. Complete the Wizard.



Note: If the Connector Agent cannot connect or cannot log in to the MailMarshal Cloud Server, you will not be able to create user groups.

To create a Connector:

1. On the main window of the Connector Agent, click **New** at bottom left to start the New Connector Wizard.
2. On the Connector Type window, choose the type of directory that this connector will use as a source (Microsoft Active Directory, a LDAP directory type, or text file). Click **Next**.
3. On the LDAP Server and Logon window, or the Microsoft Active Directory window, enter the information required to access the directory server. See Help for details. Click **Next**.
4. If you are connecting to an LDAP server, on the Search Root window enter or search for a root. See Help for details. Click **Next**.
5. On the Reload Schedule window, set the schedule on which Connector Agent will check and update groups from a connector. See Help for details. Specify the interval by choosing one of the options and then click **Next**.



Note: A minimum allowed interval for group updates applies. This interval also affects on demand requests. If you request updates more often, the updates will be refused and logged as "Update Interval Error" in the MailMarshal Cloud Customer Interface. The minimum interval is shown on the main page of the Agent. The Reseller can allow more frequent updates (Test Mode).

6. Additional windows might display to allow you to customize the connector. In most cases you can accept the default values. See Help for usage details of these windows. Click **Next** to continue.
7. On the Connector Name and Description window, enter information to identify the connector.
8. Click **Next**.
9. On the Completing window, review the connector information and then click **Finish** to create the connector.

To select User Groups from a Connector:

1. On the main window of the Connector Agent, select a Connector from the list, and then click **New** on the User Groups tab to start the New User Group Wizard.
2. On the Import User Groups window, enter the group names. Click **Browse** to view available groups.
3. Click **Next**, and then **Finish** to add the group.
4. When you have added all groups from a connector, on the main window of the Connector Agent, click **Apply** to save the changes.

5.2 Changing the Connector Agent Settings

Occasionally you may need to make changes to Connector Agent settings.

To edit connection and upgrade settings:

1. On the main window of the Connector Agent, select **File > Agent Properties**.
2. On the tabs of the Agent Properties window you can change the web URL and login, proxy settings, and automatic upgrade setting.

To edit Connectors and Groups:

1. On the main window of the Connector Agent, select a Connector from the list.
2. Review the User Groups, Connector, and directory server information using the tabs at the right.
 - On the User Groups tab, right-click a group in the list to review its properties and status.
 - On the Connector tab, select an update interval. Depending on configuration settings, you may be able to request an immediate update to the user group membership.



Note: A minimum allowed interval for group updates applies. This interval also affects on demand (Update Now) requests. If you request updates more often, the updates will be refused and logged as "Update Interval Error" in the MailMarshal Cloud Customer Interface. The minimum interval is shown on the main page of the Agent. The Reseller can allow more frequent updates (Test Mode).

Remember to apply any changes using the **Apply** button.



Note: If you delete groups in the Agent, they will not be synchronized to the MailMarshal Cloud server. However, the groups are not automatically deleted from MailMarshal Cloud. Use the MailMarshal Cloud Customer Interface to review and delete User Groups.

To enable or disable the Connector Agent:

1. At the top of the main window of the Connector Agent, the agent status (stopped or started) displays.
2. Click **Stop** or **Start** to stop or start the Agent.

5.3 Monitoring Connector Agent Activity

You can view a record of Connector Agent activity, including group creation and group updates, through the Customer Interface. See the menu item **Management > Audit History > Connector Agent Audit History**. For details of the available information, see Help for this item.

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 Fusion® 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>.