Trustwave®

CUSTOMER GUIDE

Trustwave MailMarshal Cloud

July 2021

Legal Notice

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

www.trustwave.com/support/

Trademarks

Formatting Conventions

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

Format and Symbols	Meaning
Crimson Underline	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
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

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

The Customer Web Console 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.

Trustwave 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 Trustwave MailMarshal Cloud components, see "Definitions" on page iv.

2 Understanding Trustwave MailMarshal Cloud Administration

Trustwave 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.

Trustwave 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 36.

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 Understanding the Customer Console

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

2.1.1 Logging in to the Customer Console

To access the Trustwave MailMarshal Cloud Web Console, use a current supported version of a major Web browser:

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

Note: You can connect using other browsers, and you may be able to access many functions, but only the browsers named above are tested and supported.

Access to the Web Console 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 Administration Web Console, or Trustwave.

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

2.1.2 Customer Console Features

The Web Console features a main menu at the top, with drop-down listings of items. Selecting an item usually opens a related content page.

- Most pages include a Help link at the top right. 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.
  - You can usually sort the list by clicking column headers.
  - Many lists include a Filter box at the top right. You can enter text in this box to limit the results returned.
  - You can make changes to an item using the controls in the table row.
  - For rules and rule elements, you can add new items using buttons at the top right.
  - For message history, you can take action on multiple items by checking boxes and using the action buttons at the top of the list.

Where a feature has a range of options, clicking a link displays the options on a pop-up window. Enter or select options and then click **OK** to return to the parent window. Most pop-ups include detailed Help for the fields and options.

2.2 Understanding Wildcard Characters

You can use wildcard characters in Message History searches (see “Message History” on page 12) and User Group entries (see “IP Groups” on page 26). Trustwave 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 *but not* maila.ourcompany.com
`mail[!0-9].ourcompany.com`	mails.ourcompany.com *but not* mail3.ourcompany.com

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

Spam Management

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

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

Dashboard

Shows a graphical summary of message processing and classifications for the current day, as well as information about queued messages and product features.

Notifications

Provides the latest news and updates about the Trustwave MailMarshal Cloud system.

Message History

Allows you to perform a search for messages or history records in the message database.

Message Queues

Shows the status of incoming and outgoing messages for each server and for each destination route (email domain or forwarding server).

Reports

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

Administration

Allows you to view and configure general features of the Trustwave MailMarshal Cloud interface and email filtering. These include:

- **Audit History:** Review Trustwave MailMarshal Cloud console activity, and changes to Trustwave MailMarshal Cloud configuration, for any period.
- **Connector Agent History:** Review Trustwave MailMarshal Cloud Connector Agent activity, and changes to Connector Agent configuration. This item is present if Connector Agent is enabled.
- **Domains:** Review the email domains that Trustwave MailMarshal Cloud manages for you. If permitted, you can change delivery information for a domain.
- **Configuration:** View and edit contact information for the customer (if permitted).
- **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.
- **Logins:** List and manage web console logins for your domains.

- **Message Digests:** Manage periodic notification to users of quarantined messages.
- **SQM Configuration:** Manage the web-based end user management module of Trustwave MailMarshal Cloud.

3.1 Notifications

Notifications provide important information about Trustwave 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 Console 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.

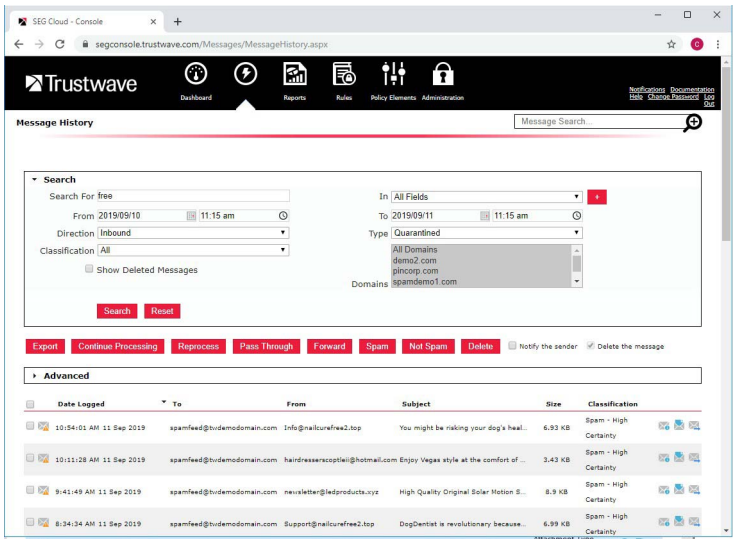
3.2 Message History

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 Web console 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.

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

Notes:

- You can use wildcard characters in the Search For text. For details, see Help.
- You can add more search criteria by clicking the + icon at the right of these fields.

- **From:** Specify the earliest time and date to search.
- **To:** Specify the latest time and date to search.
- **Direction:** Specify the message direction (inbound or outbound) or all.
- **Type:** Specify the record type(s) to search.
- **Classification**: Specify the classification to search.
- **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.
- **Show deleted messages**: Include in the results messages that have already been processed.

3.2.1 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 Web Console login.

To take action on one or more messages, select the messages using the checkboxes, and use the buttons (**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.

Tip: If the search returns more than one page of results, expand the **Advanced** section and use **For all messages, do** to take action on every message on all pages. This action uses the settings of the notify and delete checkboxes above. You will be asked to confirm the action. *Use this option with care.*

- Click the **Message Information** icon to see detailed information about a message.
- Click the **Message Viewer** icon to see the message content and processing logs (if available) and reprocess or continue processing a quarantined message.
- Click the **Handling Info** icon to see details of any manual processing actions that have been taken on a message.
- To export a basic view of the list as a CSV file, click **Export**.
- To search again, click the **Search** region to show the form.

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

3.3 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 Web console 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.

- **Search For:** Specify the text to search for. Leave blank to find all messages.
- **In:** Specify the address part to search. Only the from and to addresses (or domains) are available in this search.

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:** Specify the earliest time and date to search.
- **To:** Specify the latest time and date to search.
- **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.

3.4 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.

- Click **Process Now** to force Trustwave MailMarshal Cloud to retry delivery to the route.
- Click **Delete All** to delete all pending messages for the route.
- Expand a route (click the **+** at the left of the route name) to see a list of all messages for the route. In the details listing you can take action on individual messages.

- If you want to delete multiple messages from all routes and servers, click **Delete Messages** to select the messages you want to delete. You can select messages matching a combination of sender, recipient, and exact subject.

3.5 Reports

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

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

3.5.1 Reports on Demand

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

To run a report:

1. In the Web Console, expand **Reports**.
2. Select **Messages** or **Summary reports**.
3. In the right pane, select a report from the list, and then click **Next.**
4. If required, enter parameters to limit the report data, and then click **Submit.** 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 Web Console. 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.

3.5.2 Scheduled Reports

Any Trustwave 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 Web Console, expand **Reports > Scheduled Reports.**
2. Click **New Scheduled Report.**
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 Web Console.

To edit or delete a scheduled report:

1. In the Web Console, expand **Reports > Scheduled Reports.**
2. Choose an action using the buttons:
   a. To enable or disable scheduled generation of the report, use the **Yes/No** control in the **Enabled** column for each report**.**
   b. To delete the report, click **Delete** **.**
   c. To edit the report, click **Edit** **.** Make changes and then click **Save.**

3.6 Report Descriptions

The following types of reports are available in Trustwave MailMarshal Cloud.

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

3.6.1 Messages

These reports provide detailed data about the messages passing through Trustwave 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

3.6.2 Summary

These reports provide an overview of message traffic passing through Trustwave 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 Trustwave MailMarshal Cloud rule actions

Formats available: Text and/or Graphic

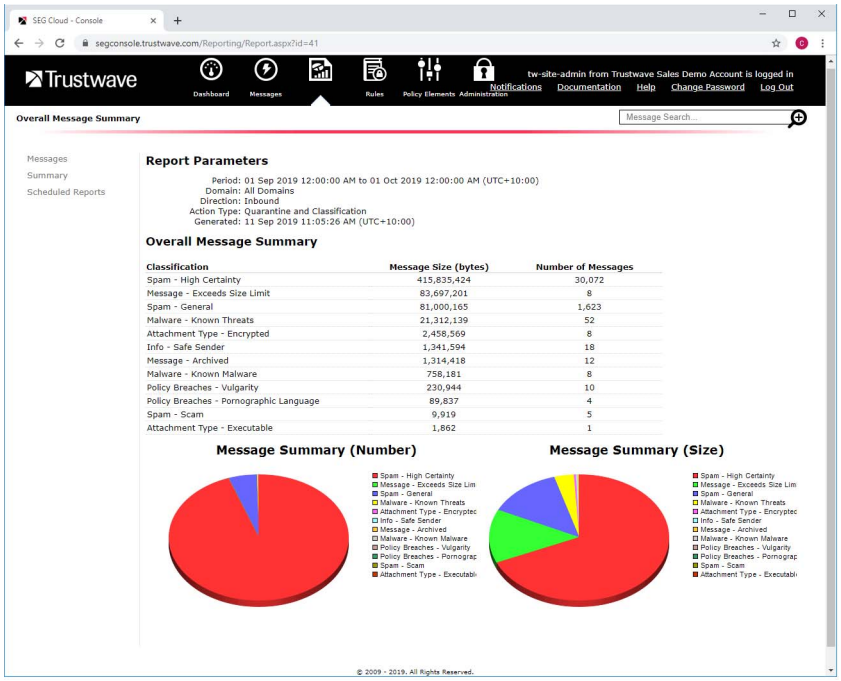
Records Returned: All

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 Received

Statistical summary of message processing during the selected period.

Formats available: Text Only

Records Returned: All

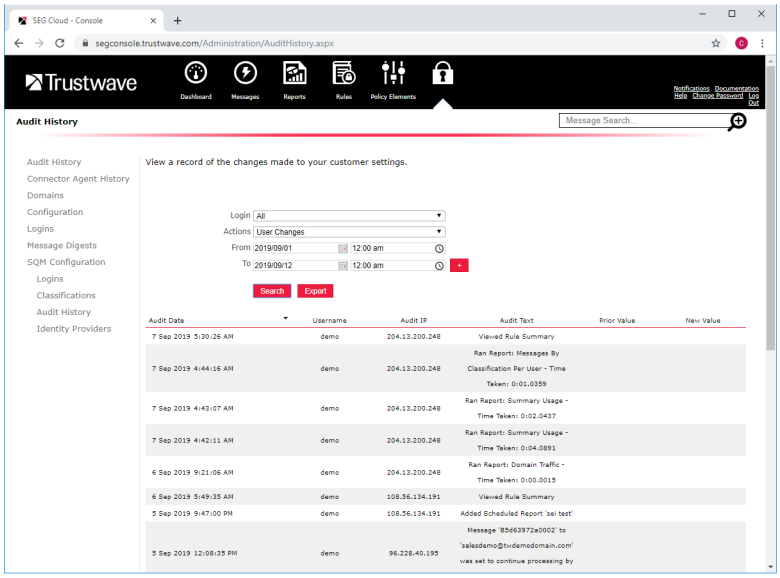
3.7 Audit History

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

To perform an Audit History search:

1. On the main menu of the Web console, select **Administration > Audit History**.
2. Enter or select parameters that define the events you want to find.
3. Click **Search**.
4. Use the links below the listing to view additional pages.
5. After you generate the Audit History, you can save it to a CSV file. To create the file, click **Export.**

For details of the available parameters, see Help.



3.8 Domains

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

For details of the columns, see Help.

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

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

If you have questions about the values listed, or you require a change in other values, contact Trustwave.

3.9 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.

3.10 Configuration

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

3.11 Logins

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

You can control each login’s access to various functions of the Trustwave MailMarshal Cloud console

To work with logins, on the main menu of the Web Console select **Administration > Logins.**

The default view shows the following columns:

- Full Name
- **User Name:** the login name for the user
- **Read Only** : Indicates whether the login has permission to make changes to settings.
- **Lock Status** : Indicates whether the login is temporarily locked because of too many invalid logon attempts.
- **Enabled:** Indicates whether the login can be used.

To add a login, click **New Login.** 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 console.

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 **Menu Security** tab.
- Email processing functions (depending on the message classification) using the **Message Security** tab.
- Email processing functions (depending on the message sender or recipient) using the **User Group Security** tab.

For details of the fields and options, see Help.

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

To unlock a login, click the **Lock** icon for the row.

To delete an existing login, click **Delete** .

To enable or disable an existing login, use the **Yes/No** control in the **Enabled** column**.**

4 Using the Customer Console for Policy Configuration

The Trustwave SEG Cloud Customer Console 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:

Rules

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.

- **Rule 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 templates, and filtering functions. Available items depend on the licensed features.

Administration

Allows you to configure notification and management of quarantined messages for email users.

- **Message Digests:** Manage periodic notification to users of quarantined messages.
- **SQM Configuration:** Manage the web-based end user management module of Trustwave SEG 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 Rules

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

4.1.1 Rule Summary

To generate a summary of rules that apply to your email, on the main menu of the Web Console select **Rules > Rule 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.

Trustwave SEG 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.

4.1.2 Customer Packages

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 **Rules > Customer Packages**. The main pane shows a list of policies.
2. To enable or disable an existing policy, use the **Yes/No** control 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, 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, use the **Yes/No** control 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.

4.1.3 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 **Rules > Disclaimers**. The main pane shows the two available disclaimers.
2. To customize a disclaimer, 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, check or clear the box for that disclaimer.

4.1.4 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 **Rules > Keywords Detection**. The main pane shows the two available detection items (inbound and outbound).
2. To customize a list of keywords and phrases, click the name link. By default the list applies to the message body.
3. To begin adding keywords, click **Add Item.**

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 30.

4. When you have finished entering or editing items, click **Save** to save changes. You can also click **Cancel** to exit without saving changes.
5. To enable or disable keywords detection for the inbound or outbound direction, check or clear the box for that direction.

4.2 User Groups

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

Each Trustwave SEG 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 9).

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. Trustwave SEG 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.

4.2.1 Creating and Maintaining User Groups

To create and maintain user groups, on the main menu of the Web console select **Policy Elements > Groups.**

To create a user group:

1. On the main menu of the Web Console, select **Policy Elements > Groups.**
2. In the right pane, click **Create a Group**.
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 **OK**.

To edit a user group:

1. On the main menu of the Web Console, select **Policy Elements > Groups.**
2. In the right pane, choose the group type by clicking a tab (Internal, External, or Connector Agent).
3. Click a group name to edit.
4. If this group was created in Trustwave SEG 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 **OK.**

4.2.2 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 Web Console, select **Policy Elements > Groups.**
2. In the right pane, choose the group type by clicking a tab (Internal or External).
3. Click the name of a group to edit the membership.
4. To add an individual address or wildcard pattern, click **Add User.** Enter the information, and then click **OK.**
5. To insert another group, click **Insert User Group.** In the new window, select a group from the list and then click **Add.**
6. To delete an address or pattern, or remove an included group, click **Delete** for the line.
7. To remove all items, click **Delete All.**
8. To import or export a text file containing email addresses, click **Import Users** or **Export Users**. 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.

4.3 IP Groups

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

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

You can include a user group within another user group.

4.3.1 Creating and Maintaining IP Groups

To create and maintain user groups, on the main menu of the Web console select **Policy Elements > Groups.**

To create an IP group:

1. On the main menu of the Web Console, select **Policy Elements > Groups.**
2. In the right pane, click the IP Groups tab.
3. Click **Create a Group**.
4. Enter a name for the group. Optionally enter a verbose description.
5. Click **OK**.

To edit an IP group:

1. On the main menu of the Web Console, select **Policy Elements > Groups.**
2. In the right pane, click the IP Groups tab.
3. Click a group name to edit.
4. You can change the name and description.
5. Click **OK.**

4.3.2 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 Web Console, select **Policy Elements > Groups.**
2. In the right pane, click the IP Groups tab.
3. Click the name of a group to edit the membership.
4. To add an individual IP address, range, or CIDR block, click **Add IP**. Enter the information, and then click **OK.**
5. To insert another group, click **Insert IP Group.** In the new window, select a group from the list and then click **Add.**
6. To delete an entry, or remove an included group, click **Delete**  for the line.
7. To remove all items, click **Delete All**.

8. To import or export a text file containing email addresses, click **Import IPs** or **Export IPs**. 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.

4.4 Message Templates

Trustwave SEG 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 Web Console, select **Policy Elements > Message Templates.**
2. Click **New Digest Template.**
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. • The recipient will be automatically provisioned as a SQM user if necessary (limited to your number of licensed users).

Table 4: Digest Template Options

Option	Results
`NORELEASE`	Do not show the message release links.
`RELEASEURL=url`	Specify the URL path to the Release web page used for this digest (see example below). Defaults to the URL of the Trustwave SEG 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.

4.5 Blended Threats Exclusions

This item allows you to maintain a list of domains that will never be rewritten for Blended Threat scanning.

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

For detail of the functionality, see Help.

4.6 Executive Names List

Trustwave SEG 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 Web Console, select **Executive Names List** (for Advanced customers, **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.

4.7 Message Digests

Trustwave SEG 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 Templates” on page 27
- 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 Web Console, on the main menu select **Administration > Message Digests.**

Tips:

- To learn more about the available options for digests, see Help for this area of the Console.
- 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 Templates” on page 27.

To create a message digest:

1. On the main menu of the Console, select **Administration > Message Digests**.
2. Click **New Digest**.
3. On the New 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. Click the digest name in the right pane of the Web Console to view its properties on a tabbed window
2. On each tab, specify the appropriate values. For more information about the fields and options, click **Help.**
3. Click **Save.**

4.8 TextCensor Scripts (Keywords Detection)

TextCensor Scripts check for the presence of text content in an email message. Trustwave SEG 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.

4.8.1 TextCensor Elements

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

4.8.1.1 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 33). 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.

4.8.1.2 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
FOLLOWEDBY `A FOLLOWEDBY[=distance] B`	The start of B occurs within *distance* words from the end of A. Returns a set of positions spanning from the start of A to the end of B. `dog FOLLOWEDBY hous*` matches `Dog in the house`
NOT FOLLOWEDBY `A NOT FOLLOWEDBY[=distance] B`	The start of B does not occur within *distance* words from the end of A. Returns a set containing the positions in A that are not followed by B. `dog NOT FOLLOWEDBY=1 hous*` matches `Dog in the house`
PRECEDEDBY `A PRECEDEDBY[=distance] B`	The end of B occurs within *distance* words from the start of A. Returns a set of positions spanning from the start of B to the end of A. `dog PRECEDEDBY cat` matches `Cat chasing dog`
NOT PRECEDEDBY `A NOT PRECEDEDBY[=distance] B`	The end of B does not occurs within *distance* words from the start of A. Returns a set containing the positions in A that are not preceded by B. `dog NOT PRECEDEDBY=2 cat` matches `Cat was not chasing dog`
NEAR `A NEAR[=distance] B`	If A occurs within *distance* words before B the resulting position spans from the start of A to the end of B. If B occurs within *distance* words before A the resulting position spans from the start of B to the end of A. `dog NEAR cat` matches `Cat chasing dog` and also matches `Dog chasing cat`
NOT NEAR `A NOT NEAR[=distance] B`	Returns the positions of all instances of A where B is not found within *distance* words from A `dog NOT NEAR=2 cat` matches `Cat was not chasing dog` and also matches `Dog was not chasing cat`

Table 5: TextCensor Positional Operators

Operator and Syntax	Matching Results
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.

4.8.1.3 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 *count* or more word positions; otherwise the result is false.

4.8.2 TextCensor Concepts

The following concepts clarify how TextCensor expressions are evaluated.

4.8.2.1 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).

4.8.2.2 Phrases

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

4.8.2.3 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`

4.8.2.4 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`

4.8.2.5 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.

4.8.2.6 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 ("\\").

4.8.2.7 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.

4.8.2.8 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.

4.8.2.9 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.

4.8.2.10 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.

4.8.3 Creating Scripts

Advanced customers can create new scripts.

1. On the main menu of the Web Console, select **Policy Elements > TextCensor Scripts**.
2. In the right pane, click **New TextCensor**
3. Enter a name for the script.
4. Optionally click **Base On** to select an existing script to be used as a template
5. Select which portions of an email message you want this script to scan by selecting one or more of the check boxes Subject, Headers, Body, and Attachments

Note: The script will check each part separately.

For instance, if you select both Headers and Message Body, the script will be evaluated once for the headers, then again for the body. Script scoring is not cumulative over the parts.

6. Select a Trigger Level. If the total score of the script reaches or exceeds this level, the script will be triggered. The total score is determined by evaluation of the individual TextCensor items in the script.
7. Add one or more TextCensor items. To begin adding items, in the TextCensor Script window click **Add Item** to open the Edit TextCensor Item window**.**
8. Enter the expression, optionally using the operators described earlier. For example:

   ```
   (Dog FOLLOWEDBY hous*) AND NOT cat
   ```

   In this example the expression score is added to the script total if the document contains the words "`dog house`" (or "`dog houses`", and so forth) in order, and does not contain the word "`cat`".

Note: TextCensor expressions are **not** case sensitive by default. However, quoted content is case sensitive. So `textcensor` would match TextCensor, but "`textcensor`" would not.

9. Click **OK** to add the expression to this script.
10. Click **Save** to save the script, or click **Cancel** to exit without saving.

4.8.4 Editing Scripts

You can change the content of an existing script, including the individual items and overall properties.

To edit a TextCensor Script:

1. In the TextCensor listing, or on the Keywords Detection page, click the script name.
2. To edit an item, click its **Edit** icon.
3. To delete an item, click its **Delete** icon.
4. Change the contents of other fields such as the script name, parts of the message tested, and trigger threshold.
5. Click **Save** to accept changes or **Cancel** to revert to the stored script.

4.9 SQM Configuration

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

The Spam Quarantine Management Website includes the following windows and features:

Log In

Allows a user to enter an email address and password to log in to the Spam Quarantine Management Website. Depending on the settings for each domain (as configured by Trustwave or the Reseller), users may be able to self-register, or you may need to import all user registrations through the Web Console. If permitted, you can set up Single Sign On with one or more SAML SSO services that you specify.

Note: Each time a user logs in with SSO, any email address aliases provided by the SSO service will be added to the list of email addresses that can be managed by the user, unless they already belong to another user. A user can also add addresses manually as described below (SSO does not delete email addresses from the list).

Home

Allows a user to view a list of email blocked since their last visit, and optionally displays summary charts of blocked and good email.

Blocked Mail

Allows a user to review a list of email quarantined in one or more classifications. The user can view, release or delete each message. The user can also add the sender address to the safe senders list (if allowed by the administrative settings). If more than one classification is available through this site, the window shows a list of classifications the user can review.

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.

Message Details

Allows a user to view the body and additional details of a message from the list of blocked email. The user can release the message or delete the message, and add the sender to safe senders.

Manage Senders

Allows a user to add, edit, or delete entries in a list of safe email addresses. Trustwave SEG Cloud uses these lists in the rule condition “Where sender is/is not in recipient’s safe senders list.”

User Settings

Allows a user to configure site and address options:

- Set the site look and feel, including language and time zone.
- Add or delete entries in a list of email addresses that they can manage using this login. Before adding a requested address to the list, Trustwave SEG Cloud requests confirmation by sending a message to the email address. The user must click a link in the message and confirm the request.
- Delegate the power to review their blocked email to one or more other users. The delegates will also be able to edit the user’s safe senders lists. The delegates can choose which user’s email to review using a list at the top of the window. Delegation is an optional feature.

- Subscribe or unsubscribe from Message Digests that list quarantined messages. This option is only available if any Digests are configured to allow users to choose subscription settings.

Change Password

Allows a user to change the password associated with their login (email address) for the SQM site.

4.9.1 Configuring SQM

- To manage SQM logins, in the Customer Web Console expand **Administration > 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.
- To manage SQM classifications, in the Customer Web Console expand **Administration > 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 Web Console expand **Administration > SQM Configuration > SQM Audit History**. For details of the available information, see Help.

4.9.2 Configuring Single Sign On for SQM

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

1. Ask Trustwave (or your Reseller) to enable SQM 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). See the MailMarshal Cloud Documentation page.
3. In the Customer Web Console expand **Administration > SQM Configuration > Identity Providers.**
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 Trustwave SEG 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 (**Administration > Configuration**) or for individual domains (**Administration > Domains**)

5 Using the Connector Agent

The Connector Agent is an optional module of Trustwave MailMarshal Cloud. To provide more flexible and effective email content security services, Trustwave 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 Trustwave 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 Trustwave MailMarshal Cloud from each connector.

Note: The Connector Agent must be able to connect to the Trustwave 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 Trustwave MailMarshal Cloud Customer Web Console server for your account.
2. Log on to the selected server. From the selected server, log in to the Customer Web Console. 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. For details of the URLs, see MailMarshal Cloud Knowledgebase Article Q21095.
   - Enter a **Login Name** (`user@domain`) and **Password** with full permission on the Customer Console 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 Trustwave 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 Trustwave MailMarshal Cloud Web Console. 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 Trustwave MailMarshal Cloud Web Console. 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 Trustwave MailMarshal Cloud server. However, the groups are not automatically deleted from Trustwave MailMarshal Cloud. Use the Trustwave MailMarshal Cloud Web Console 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 Web Console. See the menu item **Administration > Connector Agent 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 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.