Trustwave®

QUICK START GUIDE

Trustwave MailMarshal Cloud (Gateway Mode)

Trustwave MailMarshal Cloud is an email security, encryption, anti-virus and anti-spam service. MailMarshal Cloud resides outside of your network and acts as a middle-man for all email sent to or from your organization.

This Guide highlights some configuration tasks that you should consider as you prepare your new MailMarshal Cloud instance for production.

The guide also highlights common questions about daily tasks you may want to perform.

For full details of the product features and web interfaces, see the MailMarshal Cloud *Customer Guide* and the Web Console Help.

This document assumes that you have already provided Trustwave with provisioning details, and that Trustwave has provided a MailMarshal Cloud Web Console login for the first administrator. For pre-provisioning tasks, see MailMarshal Cloud Knowledgebase article Q21094, MailMarshal Cloud Pre-Provisioning Guide.

Suggested setup items:

1. **Administrative Logins**: Create additional logins to the Web Console for your authorized email administrators and help staff.
2. **Policy Review**: View the Rule Summary in the Web Console to understand the filtering options that are configured.
3. **User Groups**: Create groups for use when customizing policy. You can create groups to contain external or internal users. You can also import groups of internal users through the Connector Agent.
4. **Connector Agent**: Set up the Connector Agent in your network to synchronize internal user groups to the MailMarshal Cloud servers.
5. **Policy Customizations**: Configure policy by enabling or disabling rules, and creating user group exceptions.
    - **Set up the Executive Names List** and consider enabling additional Business Email Compromise rules. See the BEC Fraud Protection document.

6. **Self-Service Management**: Set up message digests and SQM Console users to allow end users to manage messages that are blocked as spam, or quarantined for other reasons.
7. **Mail Flow**: Set your MX records and email server forwarding to deliver messages through MailMarshal Cloud.
8. **Hardening Security Policy**: Review detection of messages that are spoofed or fail DMARC evaluation, and update policy to block these messages.

Daily administration items

Dealing with False Positives, Missed Spam, and Threat URLs: Quickly report messages that were wrongly quarantined, or not quarantined. Request classification of a URL in the Trustwave Blended Threat system.

1 Administrative Logins

Each customer account for Trustwave MailMarshal Cloud is originally provisioned with a single administrative login.

After logging in to the Web Console, you can add more administrative logins to the Console. You can set the functions of the Console that each login can access. You can choose:

- Parts of the Web Console that the login can view.
- Read Only or Read/Write access.
- Types of message actions or results the login can search for (such as quarantined or delivered messages).
- Classifications of messages within the quarantine folders that the login can view and act on.
- Groups of email users in your organization for whom the login can review and process messages.

To set up logins, in the Web Console see **Administration > Logins**.

2 Policy Review

Trustwave MailMarshal Cloud provides a number of email policy packages. Depending on the service selected, a customer will be provisioned with one or more of the following:

- **Standard Protection:** Provides scanning and control of outbound content to protect against breaches of data privacy or confidentiality.
- **Advanced Protection:** Provides real-time scanning of URL links in messages, to protect against malicious links.
- **Data Protection:** Provides scanning of outbound messages for sensitive material.
- **Acceptable Use:** Provides scanning and control of content (language and images) to help maintain a safe work environment and protect your organization’s reputation.

- **Archiving:** Provides the ability to keep a copy of messages.
- **Trustwave Secure Email Encryption:** Provides the ability to encrypt outbound messages based on email addresses or message content.

In addition, some policies are enforced for all customers.

For a full list of available policies, see the MailMarshal Cloud *Policy Guide*. To review the policy actually in force**,** in the Console see **Rules > Rule Summary**. You may also be able to customize the policies (see "Policy Customizations," below).

3 User Groups

Trustwave MailMarshal Cloud allows you to set up user groups (lists of email addresses). You can use Groups to configure custom policies for specific internal or external users.

To create and edit User Groups, in the Web Console see **Policy Elements > User Groups**.

You can also import groups of internal users through the Connector Agent.

4 Connector Agent

The Trustwave Connector Agent can synchronize user group listings from your internal network (LDAP or Active Directory services) to the cloud environment. This feature allows you to maintain filtering rules automatically – for example, a rule that blocks mail sent to invalid user addresses, or a rule that applies a special policy to a particular organizational unit.

You can download the Connector Agent from the Dashboard of the Web Console.

For details of Connector Agent installation and usage, see the Trustwave MailMarshal Cloud *Customer Guide*.

5 Policy Customizations

After reviewing the default policy and creating required User Groups, you can choose to modify Package Policy rules.

Many of the default rules can be enabled or disabled, and/or configured to apply to certain User Groups.

To customize the policy**,** in the Console see **Email Policy > Package Policies**. Click a particular package name to view a list of the included rules.

- Most package policies are permanently enabled and cannot be disabled. Most rules can be enabled or disabled.
- To enable or disable a rule, click the Yes/No slider for the specific rule.
- Most rules, as well as the Anti-Spam (Inbound) package, can be configured with user exceptions.
- To configure exceptions, click a **User Matching** link.

Note: Some basic anti-malware rules are required and cannot be disabled.

Trustwave recommends you add information to the Executive Names list to assist with fraud protection (**Policy Elements > Executive Names List**). For details of additional fraud protection options, see the *MailMarshal Cloud BEC Fraud Protection* document.

6 Self-Service Management

Trustwave MailMarshal Cloud allows you to set up self-management of quarantined email for internal recipients.

Self-service management features include the SQM Console website (Spam Quarantine Management), and periodic digests of blocked email.

6.1 SQM Setup

To set up the SQM feature:

1. Import a list of users (email addresses) that are allowed to use this site.
2. Set up a list of email classifications that can be reviewed and released by users.

In the Web Console, see **Administration > SQM Configuration**.

6.2 Digest Setup

Digests are listings of quarantined email messages. Normally, a separate digest is sent to each local email recipient if any messages addressed to them were quarantined.

To set up digests:

- Create one or more Digests. Each Digest can be sent one or more times a day. In the Web console, see **Administration > Message Digests**. You can select a template, and select which classifications to include.

7 Mail Flow

To enable MailMarshal Cloud filtering, direct all inbound and outbound email through MailMarshal Cloud.

For details of the configuration data required, see the link to your regional instance on the MailMarshal Cloud information page.

1. Configure MX records for all your local domains to point to the Trustwave MailMarshal Cloud environment:
2. Add the MailMarshal Cloud server to your SPF record.
3. Ensure that any firewalls or SMTP proxy servers are configured to allow email traffic to and from MailMarshal Cloud.

4. Set your internal email server to deliver outbound mail through MailMarshal Cloud.

8 Hardening Security Policy

Some MailMarshal Cloud security policies are in monitoring mode or disabled by default. This is to avoid blocking legitimate messages when the service is first enabled. After reviewing the results of monitoring, you should enable enforcement (blocking) by these policies.

8.1 Spoofing Detection

MailMarshal Cloud can detect spoofed messages based on your domain relay permissions and SPF records. By default, spoofing detection is in **monitoring** mode. Mail that fails the spoofing checks is logged and delivered.

After mail flow is enabled, review the results of monitoring.

- Search Mail History for incoming messages classified as **Message – Spoofed Message**
- For messages logged by the rule “Monitor Spoofed Messages”, review your list of servers allowed to relay and make any required changes.
- For messages logged by the rule “Monitor Spoofed Messages (via SPF check), review your domain SPF records and make any required changes.
- When you have made any required changes, edit the email policy to disable the Monitor roles and enable the corresponding Block rules. See **Email Policy > Package Policies > Standard Protection > Message Content (Inbound)**

8.2 DMARC Enforcement

MailMarshal Cloud can tag or block incoming messages that fail DMARC evaluation. By default, DMARC evaluation is **disabled**.

- Trustwave recommends enabling DMARC evaluation, initially in monitoring mode. See **Email Policy > Package Policies > Standard Protection > DMARC Policy (Inbound)**
- Once monitoring is enabled, messages that fail DMARC will be tagged on the message subject, and logged with a **DMARC Failed** classification. To review, search Mail History for these classifications.
- When you are satisfied that DMARC is not blocking valid messages, enable the DMARC Quarantine rules. You can make exceptions to the Quraantine rules (for known good domains that have misconfigured DMARC) with User Matching. You can leave the monitor rules enabled.

9 Daily Administration Items

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.

The following options are available to help with messages that were blocked by spam detection (or other policies) but should not be blocked, and also messages that were not properly blocked.

Some of the options allow management to be delegated to email users.

The options are listed in order from the most specific, to wider actions that could reduce anti-spam effectiveness.

9.1.1 Release and report as "not spam"

This is the best method to notify Trustwave of the issue. Customer administrators can take this action from the message history view in the management interface. For details, see MailMarshal Cloud Knowledgebase article Q20205.

- Messages reported in this way will be reviewed quickly.
- All submissions are considered and help to improve future detection. Trustwave cannot provide a personalized response to each submission. Trustwave does not guarantee change for any particular submitted message.
- This method does depend on user request or administrative monitoring.

9.1.2 Report a false negative (delivered spam):

- If the message attracted a classification, you can search for it in Message History, select it, and click **Spam**.
- If you use Office 365 you can easily deploy the Trustwave Spam Reporter Outlook plug-in for users. This plug-in allows users to report missed spam with one click. For details, see MailMarshal Cloud Knowledgebase article Q21067.
- To report a message that was delivered without attracting a classification, forward it to `spam@trustwave.com`.

If you are subscribed to Blended Threats Protection, you can report false positive and false negative URLs using a form on the Trustwave website: https://www.trustwave.com/support/submit-URL.asp

9.1.3 Additional options

For full details of the options mentioned below, see previous sections of this document and also see MailMarshal Cloud Knowledgebase article Q21199.

- **Message Digests:** You can set up digest notifications of blocked messages for users. These can be sent daily or even more frequently.
- **Spam Quarantine Management:** You can choose to allow access to the SQM web interface for end users. This site allows users to review and release messages.
- **End User "Safe" Lists:** You can choose to allow individual users to maintain a list of "safe senders". Mail to a user, sent from addresses in their "safe" list, will bypass a number of anti-spam checks.
- **Rule Exceptions:** Some rules in the Standard Protection package can have "user matching" exclusions based on the sender, recipient, or sending IP address. This option should be used with caution if other actions do not resolve the issue.

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.