QUICK START GUIDE

Trustwave SEG Cloud

Trustwave Secure Email Gateway Cloud is an email security, encryption, anti-virus and anti-spam service. SEG 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 SEG 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 SEG 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 SEG Cloud Web Console login for the first administrator. For pre-provisioning tasks, see SEG Cloud Knowledgebase article Q21094, SEG 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 SEG 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 SEG Cloud.

Daily administration items

1. **Reporting 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 SEG 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 SEG 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 SEG 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 SEG 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 SEG 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 **Rules > Customer Packages**. 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 *SEG Cloud BEC Fraud Protection* document.

6 Self-Service Management

Trustwave SEG 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 SEG Cloud filtering, direct all inbound and outbound email through SEG Cloud.

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

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

8 Daily Administration Items

SEG 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.

To quickly report a false positive:

1. In the Web Console, see **Messages > Message History**.
2. Search for the messages you want to report.
3. Select the messages and then click **Not Spam**. The messages are reported to Trustwave for automatic action and/or personal attention.

To report a false negative (delivered spam):

1. If the message attracted a classification, you can search for it in Message History, select it, and click **Spam**.
2. 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

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.