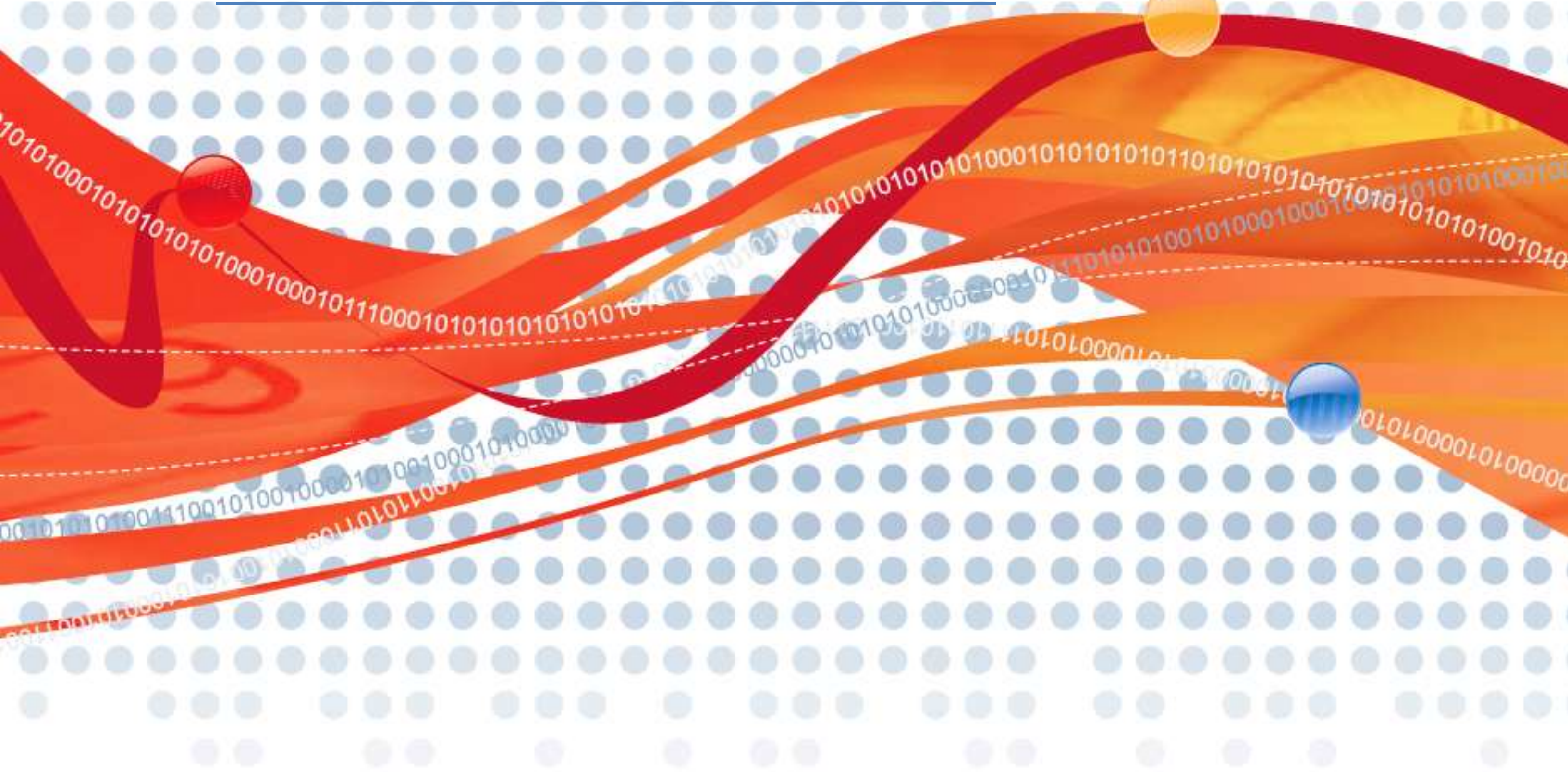
TrendMicro™
Hosted Email Security

Best Practice Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Authors : Henry Martin
Editorial : Nancy Jiang

Released : March 2018

Table of Contents

Chapter 1

1 Introduction

Trend Micro Hosted Email Security is a no-maintenance-required solution that provides continuously updated protection against threats. It uses an extensive combination of engines, patterns, heuristics, and techniques to stop spam, malware, phishing, ransomware, and advanced targeted attacks. Since it is hosted and works at the gateway level, it eliminates any potential threat before they even reach your network.

Hosted Email Security deployment is easy, requiring organizations to simply redirect their MX records. The default settings in Hosted Email Security are strategically optimized to provide immediate protection upon deployment. Configuration tweaks and changes can be done to fit the organization’s requirement and allow lots of flexibility.

This Best Practice Guide outlines the best practices when using Trend Micro Hosted Email Security to protect your mailboxes at the gateway level.

Chapter 2

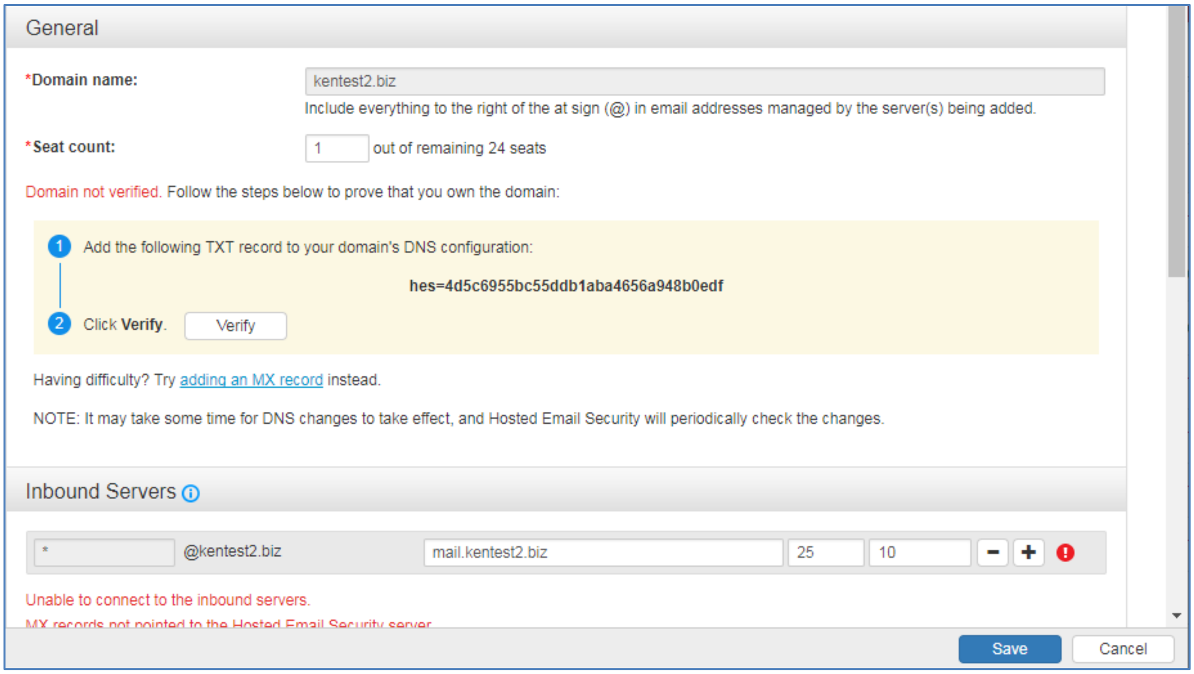
2 Hosted Email Security Provisioning

Hosted Email Security can be provisioned to work with any type of email environment. Regardless if the organization is using a traditional on-premises mail server, or their mailboxes are hosted in Office 365 or Google G Suite, Hosted Email Security is a great choice for keeping malicious email messages and attachments out of your network.

Provisioning starts with adding your domain name in the Hosted Email Security administrator console and identifying the inbound servers to where Hosted Email Security will relay all your incoming email messages. Optionally, outbound filtering can also be enabled. For details about this procedure, refer to the "Adding a Domain" section in the Administrator's Guide.

Once the domain is added, its status will show as "**Configuration Required**" in the Administrator Console. A red exclamation mark will be shown next to the field that requires your operation or reports any problem. You can hover over the exclamation mark to view the detailed error message.

To verify your domain and complete the provisioning, the provided DNS TXT record in the domain provisioning screen must be added to your DNS. Optionally, an MX record pointing to the Hosted Email Security address may be used instead.



General

*Domain name: kentest2.biz

Include everything to the right of the at sign (@) in email addresses managed by the server(s) being added.

*Seat count: 1 out of remaining 24 seats

Domain not verified. Follow the steps below to prove that you own the domain:

1 Add the following TXT record to your domain's DNS configuration:

hes=4d5c6955bc55ddb1aba4656a948b0edf

2 Click **Verify**.

Having difficulty? Try adding an MX record instead.

NOTE: It may take some time for DNS changes to take effect, and Hosted Email Security will periodically check the changes.

Inbound Servers

*	@kentest2.biz	mail.kentest2.biz	25	10

Unable to connect to the inbound servers.

MX records not pointed to the Hosted Email Security server

Refer to the “Configuring a Domain” section in the Administrator’s Guide for details about this procedure.

While the domain is in “**Configuration Required**” status, two default policies will not be editable. These are the “Virus” policy and the “Spam or Phish” policy.

It is important to note that email messages for the domain cannot be routed through Hosted Email Security while the domain status is at “Configuration Required”. Once the domain status is shown as “Completed”, then you can start using Hosted Email Security and route your email messages for filtering.

The sub-sections below outline the best practice of provisioning in various environments.

2.1 On-Premises Mail Server

After provisioning the domain in the administrator console, the next important step is to secure the mail server to ensure that no attacker can bypass Hosted Email Security scanning. To achieve this:

- Configure the firewall and/or mail server to accept email messages only from the following IP addresses:

  For the EMEA site:

  - 52.48.127.192/26
  - 52.58.62.192/26
  - 52.58.63.0/25

  For all other regions:

    - 54.86.63.64/26
    - 54.219.191.0/25

- Additionally, if the organization's firewall, MTA, or mail server is configured to check any IP Reputation/RBL service provider, the same set of IP blocks above must be added to the IP Reputation approved list. Another option is to disable the IP Reputation check on the firewall, MTA, or mail server. Hosted Email Security has its own IP Reputation/RBL list using Trend Micro's Email Reputation Service.
- Disable SPF checking on the email gateway, MTA, or mail server (if enabled). All incoming email messages will come from Hosted Email Security IP addresses after provisioning is done, causing the SPF checking to fail on the said hosts. Refer to your mail application's documentation for the exact procedure.
- If Hosted Email Security outbound filtering is used, configure the mail server to send all outgoing email messages to Hosted Email Security by configuring a smarthost. Point the smarthost/relay connector to:
    - EMEA customers: relay.hes.trendmicro.eu
    - Non-EMEA customers: relay.hes.trendmicro.com

  Check your MTA or mail server's documentation on how to make the configuration.

2.2 Office 365

For customers using Office 365, it is also necessary to configure the Inbound and Outbound Connectors to work with Hosted Email Security. These procedures are outlined in details below.

2.2.1 Configuring Inbound Connector

Configure Office 365 Inbound connectors to allow email traffic from Hosted Email Security MTAs.

***Important:** Consult the Microsoft Office 365 help for information about adding connectors. Some Office 365 plans do not offer connectors.*

http://technet.microsoft.com/en-us/library/exchange-online-mail-flow.aspx

1. Log on to your Office 365 administration center.
2. In the navigation on the left, go to **Admin > Exchange**. The Exchange admin center screen appears.
3. In the navigation on the left, go to **mail flow**, and then click **connectors** in the top navigation.
4. Do the following to add an Inbound Connector to Office 365:

   Note: By adding an inbound connector, you can configure Office 365 to accept mail filtered by Hosted Email Security for delivery to email accounts in your Office 365 managed domain.

   a. Click the plus **(+)** icon.

      A new connector configuration screen appears.

   b. In the **From** field, select **Partner organization**.

c. In the **To** field, select **Office 365**.
d. Click **Next**.
e. In the **Name** field, type a descriptive name for the connector.

For example, type **Trend Micro Hosted Email Security (Inbound)**.

f. Click **Next**.
g. Select **Use the sender's IP address**, and then click **Next**.
h. In the **Specify the sender IP address range** field, add the following Hosted Email Security IP addresses:

Europe, the Middle East, Africa

- 52.48.127.192/26
- 52.58.62.192/26
- 52.58.63.0/25

All other regions

- 54.86.63.64/26
- 54.219.191.0/25

i. Click **Next**.
j. Select **Reject email messages if they aren't sent over TLS**, and then click **Next**. The New connector confirmation screen appears, displaying all the settings that you have configured.
k. Click **Save**.

Additionally, disable SPF checking on Office 365 (if enabled). All incoming email messages will come from Hosted Email Security IP addresses after provisioning is done, causing the SPF checking to fail on the said hosts. Refer to Office 365 documents for details about the procedure.

2.2.2 Configuring Outbound Connector

When using Hosted Email Security Outbound Filtering, configure Office 365 Outbound connectors to route email traffic to Hosted Email Security MTAs.

***Important:** Consult the Microsoft Office 365 help for information about adding connectors. Some Office 365 plans do not offer connectors.*

http://technet.microsoft.com/en-us/library/exchange-online-mail-flow.aspx

1. Log on to your Office 365 administration center.
2. In the navigation on the left, go to **Admin > Exchange**. The Exchange admin center screen appears.
3. In the navigation on the left, go to **mail flow**, and then click **connectors** in the top navigation.
4. Do the following to add an Outbound Connector to Hosted Email Security:

   Note: By adding an outbound connector, you can configure Office 365 to relay outbound email messages to Hosted Email Security for filtering and delivery to recipients outside of your Office 365 managed domain.

   a. Click the plus **(+)** icon.

      A new connector configuration screen appears.

   b. In the **From** field, select **Office 365**.
   c. In the **To** field, select **Partner organization**.
   d. Click **Next**.
   e. In the **Name** field, type a descriptive name for the connector.

      For example, type **Trend Micro Hosted Email Security (Outbound).**
   f. Click **Next.**
   g. Select **Only when I have a transport rule set up that redirects messages to this connector**, and then click **Next.**
   h. Select **Route email through these smart hosts**, then click the plus **(+)** icon, and then add to the list: **relay.hes.trendmicro.eu** for EMEA region or **relay.hes.trendmicro.com** for other regions, and then click **Next**.
   i. Keep the default settings on the screen that appears, and then click **Next**. The New connector confirmation screen appears, displaying all the settings that you have configured.
   j. Click **Next**.
   k. Add an email address to the field provided, and then click **Validate**. After the validation process completes, the **Validation Result** screen displays.
   l. Click **Save**.

2.3 Google G Suite

Once your domain is activated, you can proceed in setting up the Google G Suite mail settings to work with Hosted Email Security.

2.3.1 Inbound Configuration

1. Configure the Google G Suite email settings.
   1. Log on to the Google Apps domain management portal.
      - Go to the Google sign-in page.
      - Type your administration account email addresses (including username and domain) and password.
   2. Click the **Settings** tab and select **Email** in the **Services** section.

3. Navigate to **Inbound Gateway** and enter the following IP addresses of the Trend Micro Hosted Email Security Servers:

   Europe, the Middle East, Africa

   - 52.48.127.192/26
   - 52.58.62.192/26
   - 52.58.63.0/25

   All other regions

   - 54.86.63.64/26
   - 54.219.191.0/25

2. Ensure that the **Only let users receive email from the email gateways listed above. All other mail will be rejected** checkbox is selected.

2.3.2 Outbound Configuration

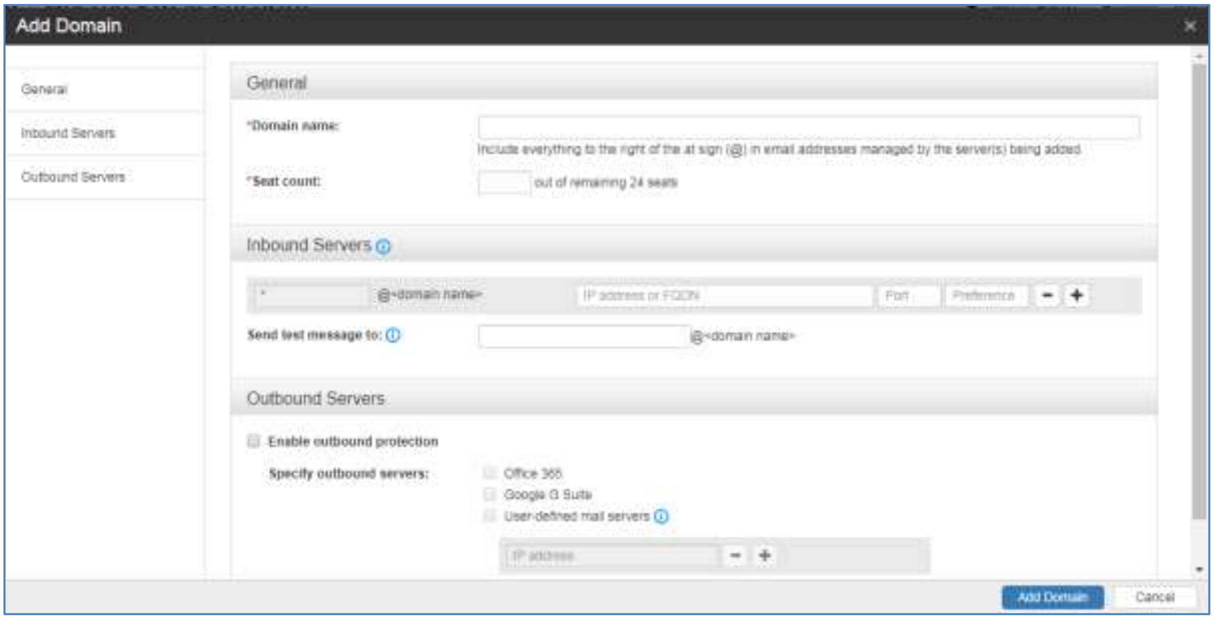
1. Log on to the G Suite Domain Management Portal.
2. Navigate to the **Settings** tab, and then select **Email** under the **Services** section.
3. Navigate to **Outbound Gateway** and enter the FQDN of Hosted Email Security as the outbound mail gateway.
   - **EMEA customers**: relay.hes.trendmicro.eu
   - **Non-EMEA customers:** relay.hes.trendmicro.com

2.4 Provisioning Additional Domains

Additional domains and even sub-domains may need to be provisioned in Hosted Email Security if the organization is also using those domains for email communication. Provisioning them so that Hosted Email Security can be used to filter email messages for all email domains, which is necessary for the organization to have the best and most secure protection.

To provision additional domains:

1. Log on to the Hosted Email Security administrator console.
2. Go to the **Domains** tab.
3. Click the **Add** button.
4. Fill in the required details and click **Add Domain**.

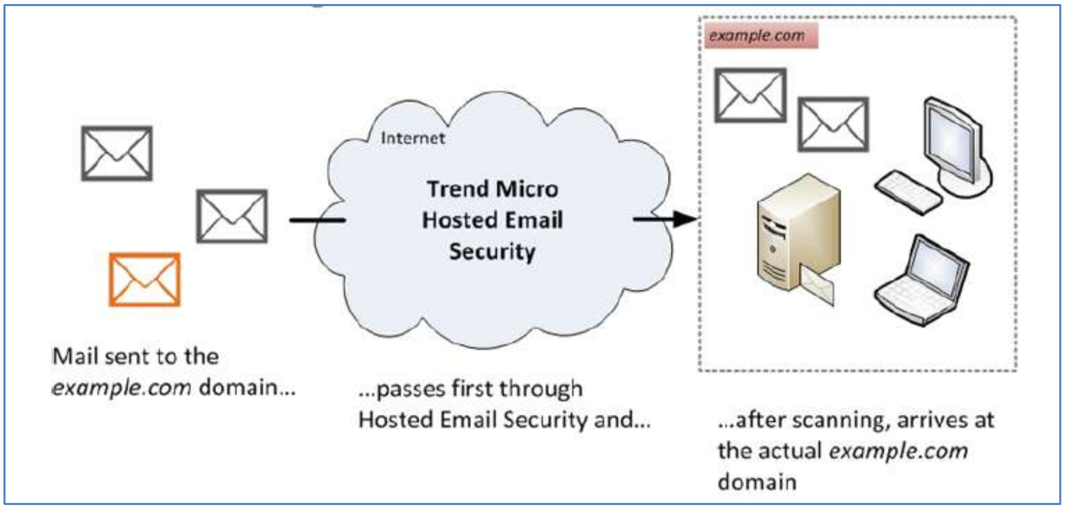


Include everything to the right of the at sign (@) in email addresses managed by the server(s) being added

5. Configure the required DNS TXT record or MX record to complete domain provisioning.

3 Inbound Mail Protection

Once Hosted Email Security is completely provisioned, email traffic will flow according to the diagram below.


example.com
Internet
Trend Micro Hosted Email Security
Mail sent to the *example.com* domain...
...passes first through Hosted Email Security and...
...after scanning, arrives at the actual *example.com* domain

1. The originating MTA performs a DNS lookup of the MX record for “example.com” to determine the location of the” example.com” domain.

   The MX record for “example.com” points to the IP address of the Hosted Email Security MTA instead of the original “example.com” Inbound Server.

2. The originating MTA routes messages to Hosted Email Security.
3. The Hosted Email Security MTA accepts the connection from the originating mail server.
4. Hosted Email Security performs IP reputation-based filtering at the MTA connection level to decide on an action to take. Actions include the following:

   - Hosted Email Security terminates the connection, rejecting the messages.
   - Hosted Email Security accepts the messages and filters them using content-based policy filtering.

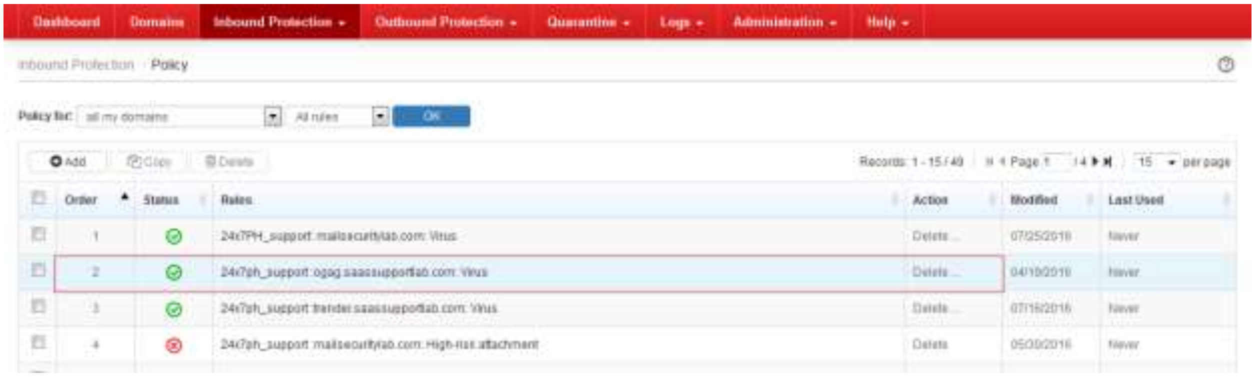
5. Hosted Email Security examines the message contents to determine whether the message contains malware such as a virus, or if it is spam, and so on.
6. Assuming that a message is slated for delivery according to the domain policy rules, the Hosted Email Security MTA routes the message to the original example.com Inbound Server.

Inbound Mail Protection best practice includes enabling and configuring protection against different types of threats such as malware, spam, spoofed email messages, and even ransomware.

3.1 Malware and 0-Day Threats Protection

By default, the virus policy is already set to “quarantine”, but if it was modified to a different action other than “delete”, set it back to “delete” or “quarantine” to avoid any malware entering your system.

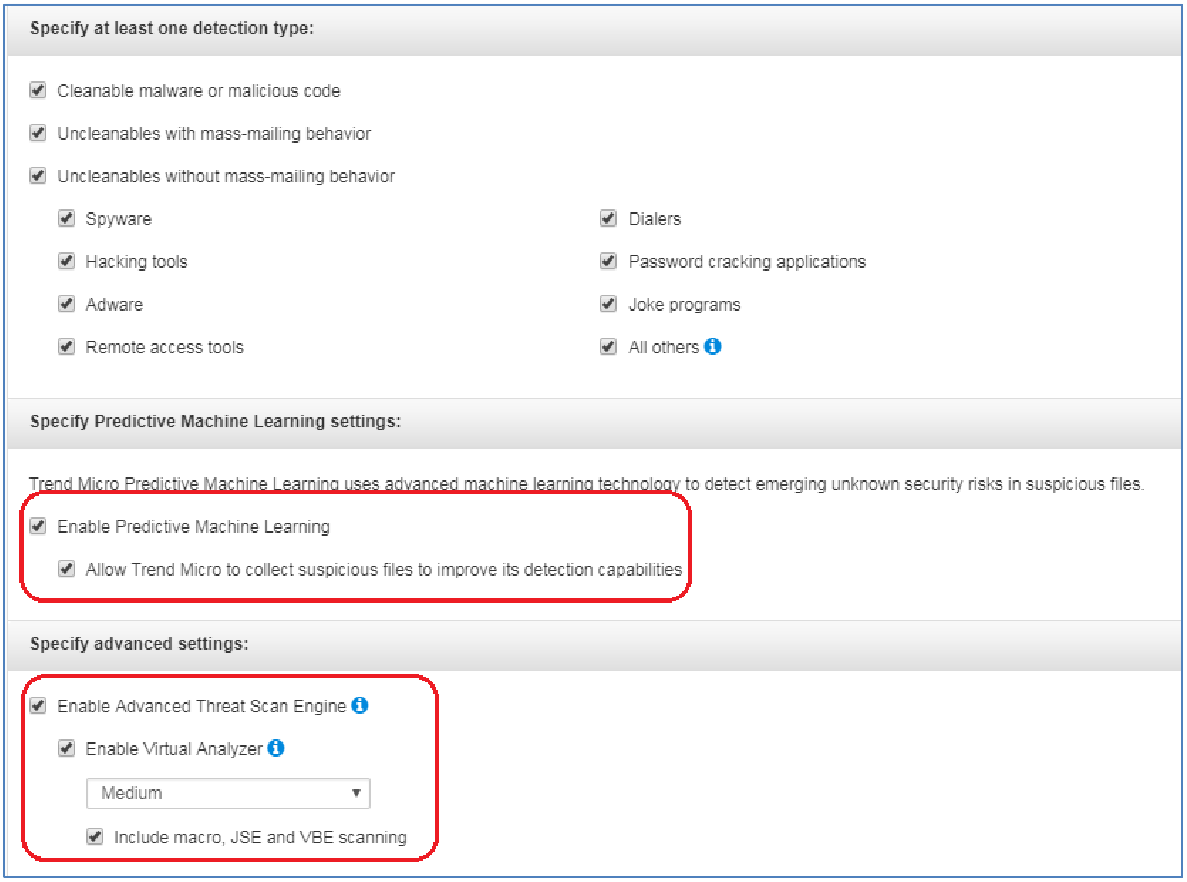
1. Log on to the Hosted Email Security administrator console.
2. Go to **Inbound Protection** > **Policy** and look for the **Virus** policy.



Policy for: all my domains · All rules · 15 per page

Order	Status	Rules	Action	Modified	Last Used
1	✓	24x7PH_support: mailsecuritylab.com: Virus	Delete ...	07/25/2016	Never
2	✓	24x7ph_support: ogag.saassupportlab.com: Virus	Delete ...	04/19/2016	Never
3	✓	24x7ph_support: trender.saassupportlab.com: Virus	Delete ...	07/16/2016	Never
4	⊗	24x7ph_support: mailsecuritylab.com: High-risk attachment	Delete	05/30/2016	Never

3. Make sure the action is set to “delete” or “quarantine.”
4. Ensure that the policy applies to “ALL users”, and there are no “Senders and Recipients Exceptions”.
5. Under **Scanning Criteria**, click on **malware or malicious code**.
6. Ensure all malware detection types are checked.
7. Enable Advanced Threat Scan Engine, Virtual Analyzer, and **Include macro and script scanning**. This provides protection against zero-day and unknown threats by running suspicious files on a sandbox environment.
8. Enable Predictive Machine Learning and **Allow Trend Micro to collect suspicious files to improve its detection capabilities**.



Specify at least one detection type:

☑ Cleanable malware or malicious code

☑ Uncleanables with mass-mailing behavior

☑ Uncleanables without mass-mailing behavior

☑ Spyware

☑ Hacking tools

☑ Adware

☑ Remote access tools

☑ Dialers

☑ Password cracking applications

☑ Joke programs

☑ All others ℹ

Specify Predictive Machine Learning settings:

Trend Micro Predictive Machine Learning uses advanced machine learning technology to detect emerging unknown security risks in suspicious files.

☑ Enable Predictive Machine Learning

☑ Allow Trend Micro to collect suspicious files to improve its detection capabilities

Specify advanced settings:

☑ Enable Advanced Threat Scan Engine ℹ

☑ Enable Virtual Analyzer ℹ

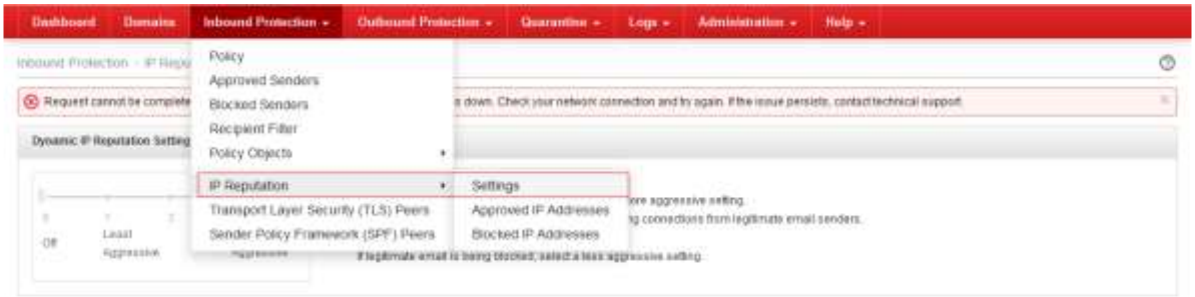
Medium ▾

☑ Include macro, JSE and VBE scanning

3.2 Spam Protection

3.2.1 Configure IP Reputation Setting

a. Go to **Inbound Protection** > **IP Reputation** > **Settings**.



Request cannot be complete … s down. Check your network connection and try again. If the issue persists, contact technical support.

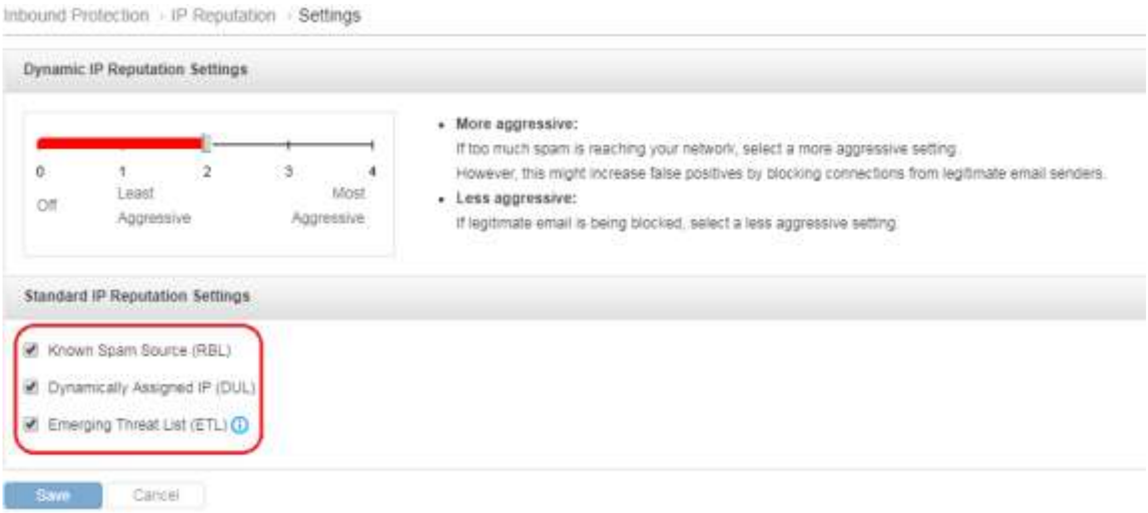
…ore aggressive setting.

…g connections from legitimate email senders.

If legitimate email is being blocked, select a less aggressive setting.

b. Set the aggressiveness level based on your organization needs. If you are constantly under attack, increasing the aggressiveness level is recommended.

c. Enable all 3 IP Reputation checks (RBL, DUL, and ETL)


Inbound Protection › IP Reputation › Settings

Dynamic IP Reputation Settings

- **More aggressive:**
  If too much spam is reaching your network, select a more aggressive setting.
  However, this might increase false positives by blocking connections from legitimate email senders.
- **Less aggressive:**
  If legitimate email is being blocked, select a less aggressive setting.

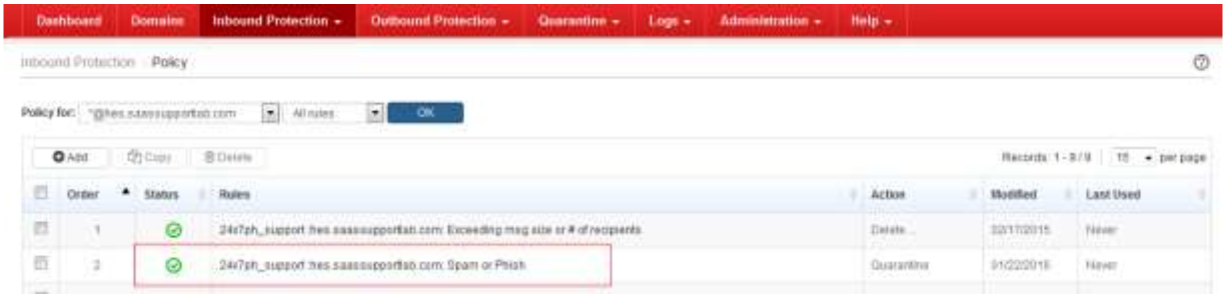
Standard IP Reputation Settings

☑ Known Spam Source (RBL)
☑ Dynamically Assigned IP (DUL)
☑ Emerging Threat List (ETL)

3.2.2 Add filters to default spam and phish policy

Depending on the amount of spam messages your organization is getting, it may be necessary to increase the spam detection level, enable social engineering attack and include advanced analysis to identify threats.

1. Log on to the Hosted Email Security administrator console.
2. Go to **Inbound Protection** > **Policy** and look for the Spam or Phish policy for each managed domain.

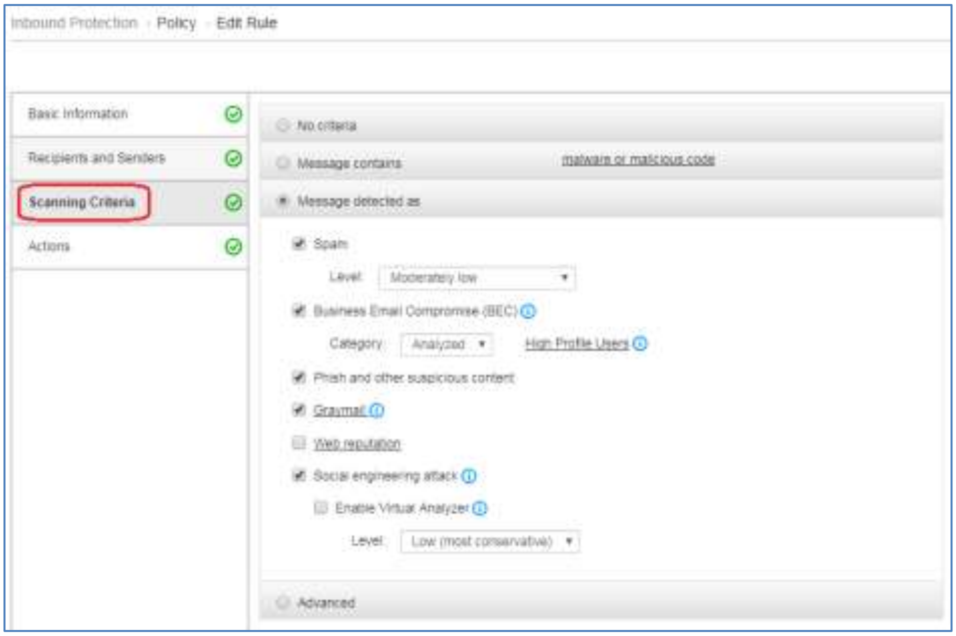


Policy for: *@hes.saassupportlab.com All rules

Records: 1 - 9 / 9 15 per page

☐	Order	Status	Rules	Action	Modified	Last Used
☐	1	✓	24x7ph_support hes.saassupportlab.com: Exceeding msg size or # of recipients	Delete ...	02/17/2015	Never
☐	2	✓	24x7ph_support hes.saassupportlab.com: Spam or Phish	Quarantine	01/22/2015	Never

3. Click **Scanning Criteria**.



Inbound Protection › Policy › Edit Rule

Basic Information ✓

Recipients and Senders ✓

Scanning Criteria ✓

Actions ✓

○ No criteria

○ Message contains malware or malicious code

● Message detected as

☑ Spam

Level: Moderately low ▾

☑ Business Email Compromise (BEC) ⓘ

Category: Analyzed ▾ High Profile Users ⓘ

☑ Phish and other suspicious content

☑ Graymail ⓘ

□ Web reputation

☑ Social engineering attack ⓘ

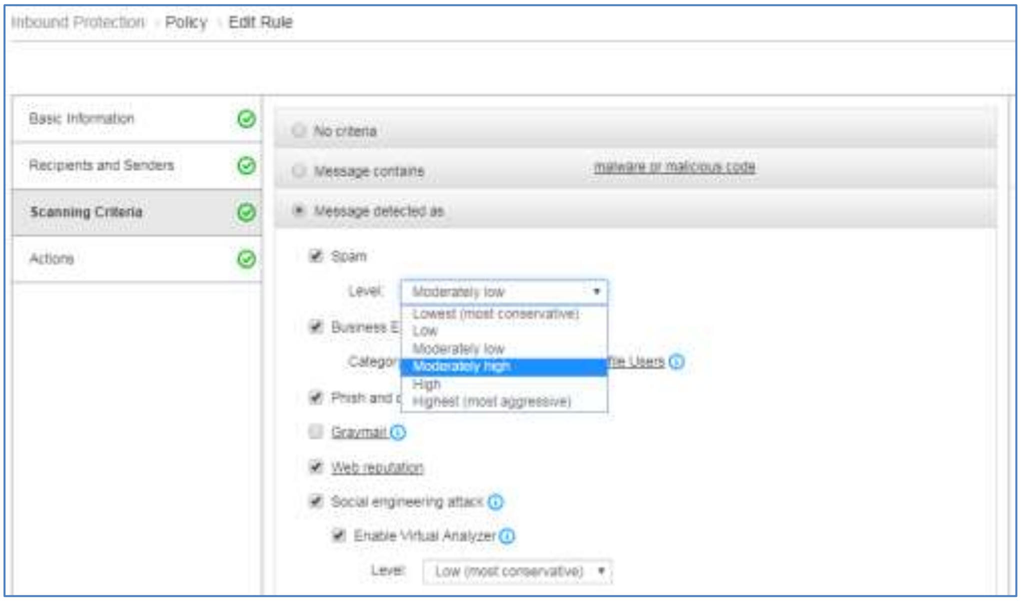
□ Enable Virtual Analyzer ⓘ

Level: Low (most conservative) ▾

○ Advanced

4. Check all boxes, except Graymail, and set Spam check to a higher level. Graymails are covered by a different policy, “Newsletter or spam-like”.

   Note that setting spam check higher might lead to more false positives, but it can also reduce false negative messages and avoid malicious messages in.



Inbound Protection › Policy › Edit Rule

Basic Information ✓

Recipients and Senders ✓

Scanning Criteria ✓

Actions ✓

○ No criteria

○ Message contains malware or malicious code

● Message detected as

☑ Spam

Level: Moderately low ▾

Lowest (most conservative)
Low
Moderately low
Moderately high
High
Highest (most aggressive)

☑ Business E

Categor ...file Users ⓘ

☑ Phish and c

□ Graymail ⓘ

☑ Web reputation

☑ Social engineering attack ⓘ

☑ Enable Virtual Analyzer ⓘ

Level: Low (most conservative) ▾

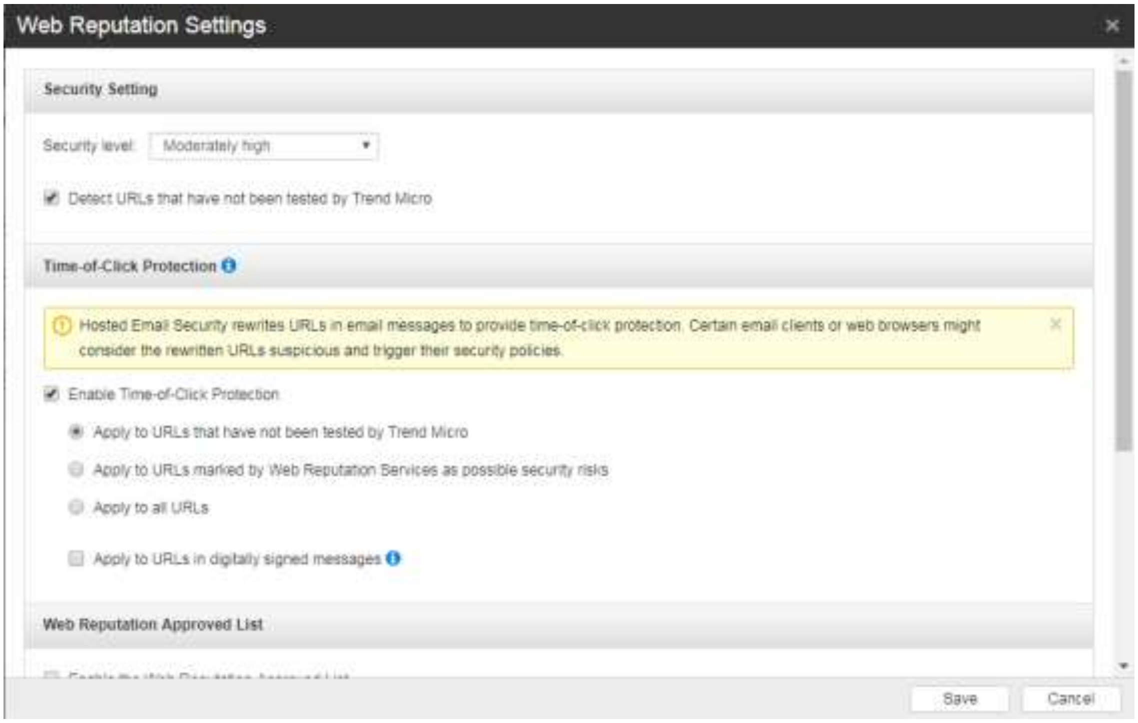
***Note*:**
If Virtual Analyzer is enabled, Hosted Email Security performs observation and analysis on samples in a closed environment. Advanced analysis can delay the delivery of messages by 5 to 30 minutes.

3.2.3 Enable Time-of-Click Protection

Working in conjunction with Web Reputation filter, Time-of-Click protection rewrites URL's in email messages for further analysis. Trend Micro analyzes those URL's at the time of click and will block them if they are malicious to protect the users.

To enable Time-of-Click Protection, go to **Inbound Protection > Policy > Spam or Phish policy > Scanning Criteria > Web Reputation** page. Select to enable the options:

- Detect URLs that have not been tested by Trend Micro
- Enable Time-of-Click Protection
- Apply to URLs that have not been tested by Trend Micro



Web Reputation Settings

Security Setting

Security level: Moderately high ▾

☑ Detect URLs that have not been tested by Trend Micro

Time-of-Click Protection

Hosted Email Security rewrites URLs in email messages to provide time-of-click protection. Certain email clients or web browsers might consider the rewritten URLs suspicious and trigger their security policies.

☑ Enable Time-of-Click Protection

● Apply to URLs that have not been tested by Trend Micro

○ Apply to URLs marked by Web Reputation Services as possible security risks

○ Apply to all URLs

□ Apply to URLs in digitally signed messages

Web Reputation Approved List

See Configuring Time-of-Click Protection Settings

3.2.4 Enable the Newsletter or Spam-Like Policy

Hosted Email Security includes a default policy named “Newsletter or spam-like”. This policy scans specifically for Graymail, which refers to unsolicited bulk email messages that are not spam. This policy should be enabled and a scan action configured based on the organizations’ need or preference. Some organizations prefer to allow newsletters to pass through while some do not.

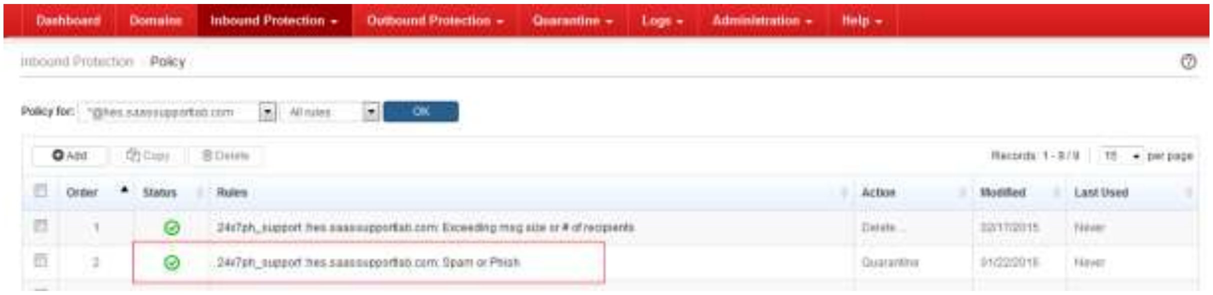
3.3 Spoofed Email Protection

Hosted Email Security has multiple technologies to help protect against spoofed email messages. Each of these is described in details below.

3.3.1 Enable Spoofed Email Filters in Spam or Phish Policy

Email Spoofing is used on all sorts of phishing and social engineering attacks. By enabling these default filters in Hosted Email Security, tighter protection can be implemented.

1. Log on to the Hosted Email Security administrator console.
2. Go to **Inbound Protection** > **Policy** and look for the Spam or Phish policy for each managed domain.

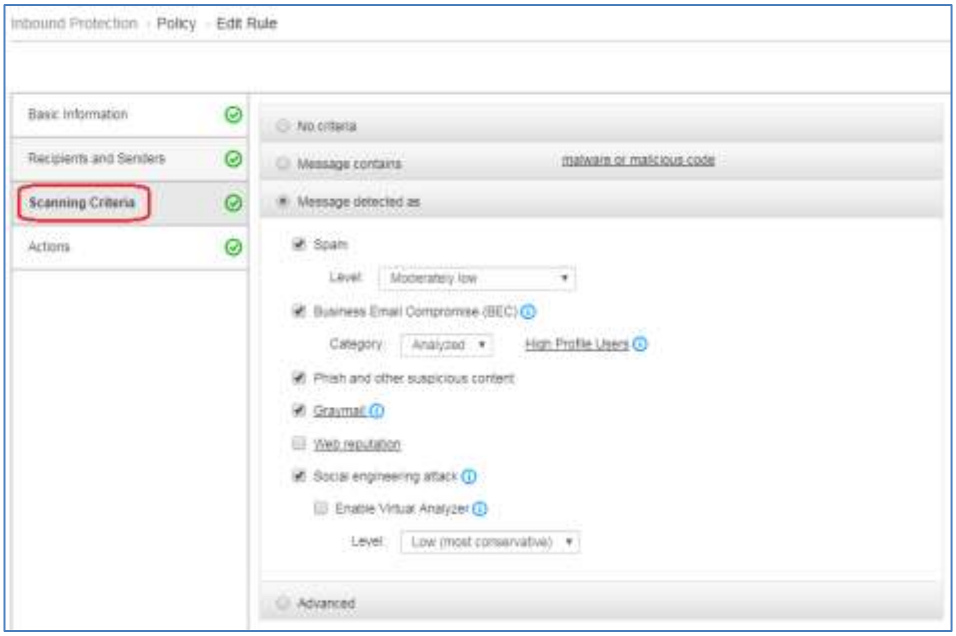


Policy for: *@hes.saassupportlab.com All rules

Records: 1 - 9 / 9 15 per page

☐	Order	Status	Rules	Action	Modified	Last Used
☐	1	✓	24x7ph_support hes.saassupportlab.com: Exceeding msg size or # of recipients	Delete ...	02/17/2015	Never
☐	2	✓	24x7ph_support hes.saassupportlab.com: Spam or Phish	Quarantine	01/22/2015	Never

3. Click **Scanning Criteria**.



○ No criteria

○ Message contains malware or malicious code

● Message detected as

☑ Spam

Level: Moderately low

☑ Business Email Compromise (BEC)

Category: Analyzed High Profile Users

☑ Phish and other suspicious content

☑ Graymail

☐ Web reputation

☑ Social engineering attack

☐ Enable Virtual Analyzer

Level: Low (most conservative)

○ Advanced

4. Check to enable the boxes for Business Email Compromise (BEC), Phish and other suspicious content, and Social Engineering Attack.

5. Under **Social engineering attack**, select the **Enable Virtual Analyzer** check box.

> ***Note***:
> ***If Virtual Analyzer is enabled, Hosted Email Security performs observation and analysis on samples in a closed environment. Advanced analysis can delay the delivery of messages by 5 to 30 minutes.***

3.3.2 Configure the list of "High-Profile Users" for BEC filter

Business Email Compromise (BEC) is a type of spoofed email attack that aims to compromise official business email accounts to conduct unauthorized fund transfers. A BEC scam is a form of phishing attack where a fraudster impersonates a high profile executive, for example, the CEO or CFO, and attempts to trick an employee, a customer, or a vendor into transferring funds or sensitive information to the fraudster.

By identifying the names of these High-Profile Users in Hosted Email Security, it can provide tighter security for email messages claiming to be from those users.

See Configuring High Profile Users.

3.3.3 Create an anti-spoof policy

Create a policy for filtering spoofed email messages from the same domain as recipients.

> ***Note***:
> Normal spoofed email messages spoof the recipient domain. Best practice is to have internal email messages not be routed out of the Internet or through Hosted Email Security. Create a policy to filter email messages coming from your own domain.

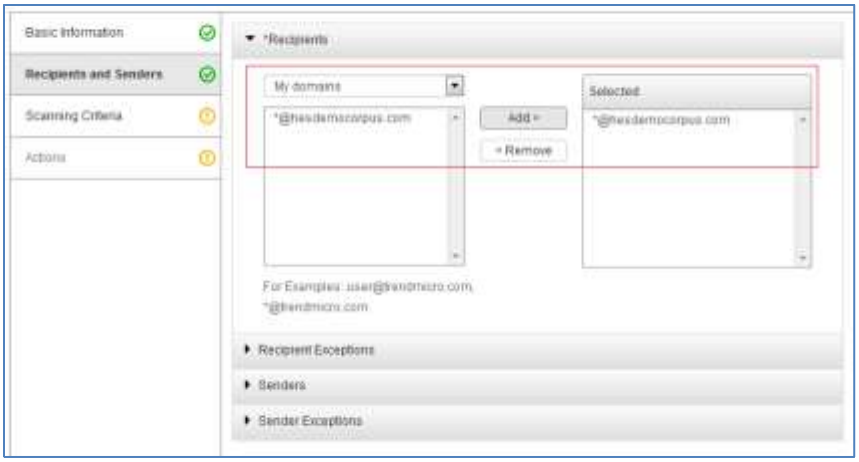
> ***Warning***:
> *Make sure inter-domain email messages are not routed to the Internet.*

a. On your browser, log on to the Hosted Email Security administrator console.

b. Go to **Inbound Protection > Policy** and click **Add**.

c. Type name of the rule you are creating.

d. Under **Recipients and Senders > Recipients**, add your domain.



My domains

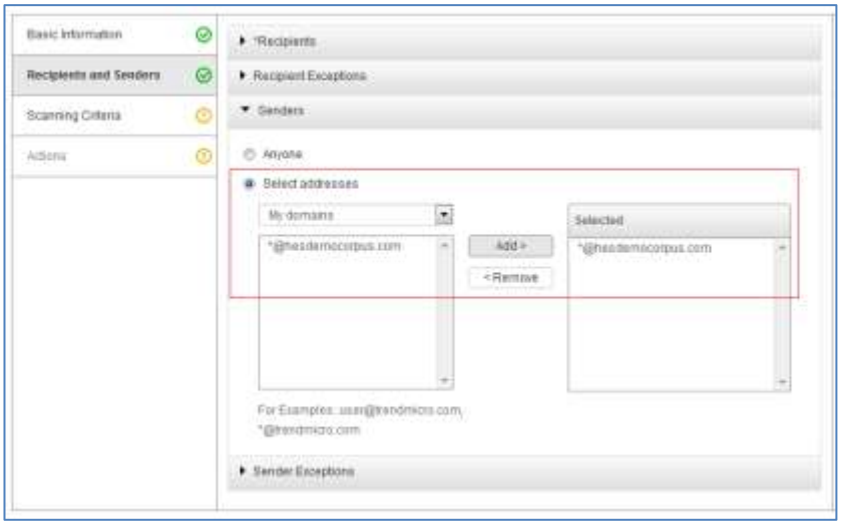
*@hesdemocorpus.com

Selected

*@hesdemocorpus.com

For Examples: user@trendmicro.com, *@trendmicro.com

e. Under **Recipients and Senders > Senders**, add the same domain.



○ Anyone

● Select addresses

My domains

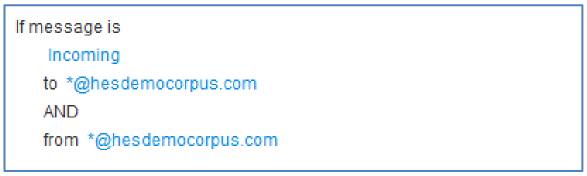
*@hesdemocorpus.com

Selected

*@hesdemocorpus.com

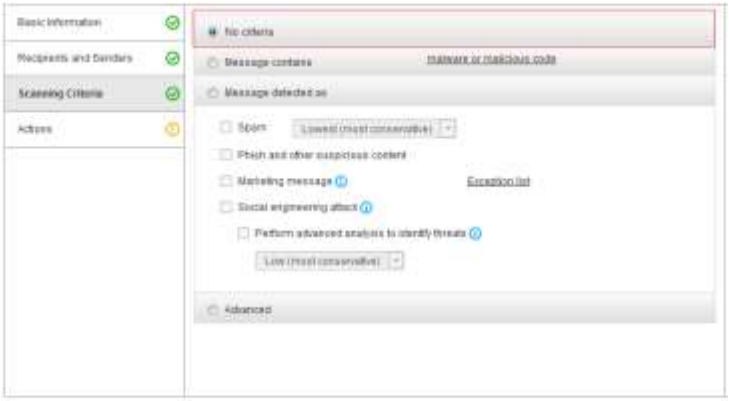
For Examples: user@trendmicro.com, *@trendmicro.com

f. The setting will be similar to below.



If message is
Incoming
to *@hesdemocorpus.com
AND
from *@hesdemocorpus.com

g. Under **Scanning Criteria**, select **No Criteria**. So any email message coming in to Hosted Email Security from your domain and going to your same domain will be filtered.



● No criteria

○ Message contains malware or malicious code

○ Message detected as

□ Spam Lowest (most conservative)

□ Phish and other suspicious content

□ Marketing message Exception list

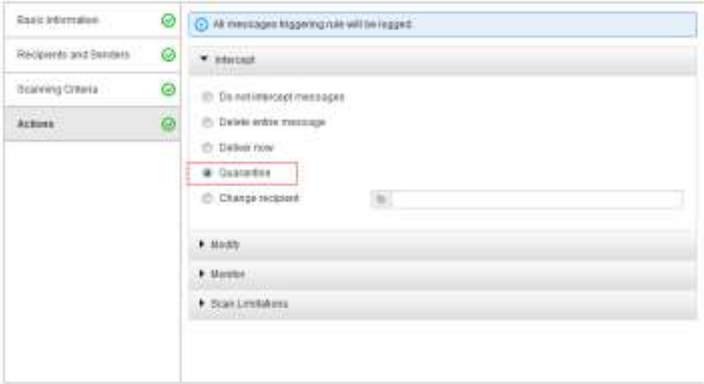
□ Social engineering attack

□ Perform advanced analysis to identify threats

Low (most conservative)

○ Advanced

h. Under **Actions**, select “quarantine” so that you can still review filtered email messages.



All messages triggering rule will be logged.

○ Do not intercept messages

○ Delete entire message

○ Deliver now

● Quarantine

○ Change recipient

i. Click **Submit**.

3.3.4 Enable SPF Checking

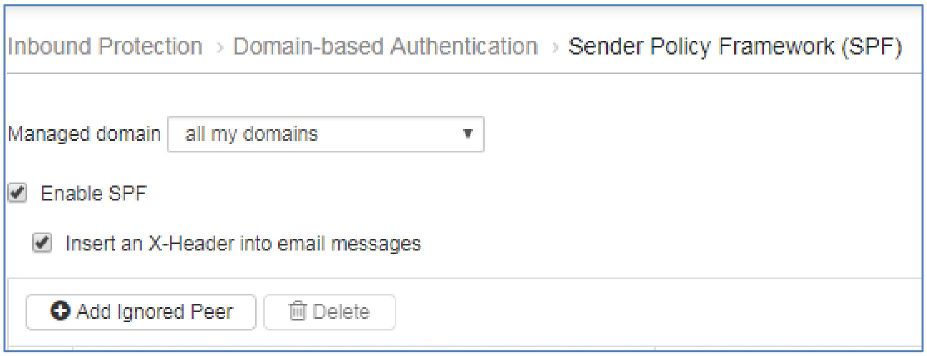
SPF is an open standard to prevent sender address forgery. SPF protects the ***envelope sender address*** that is used for the delivery of messages. Hosted Email Security enables you to configure SPF to ensure the sender's authenticity.

SPF requires the owner of a domain to specify and publish their email sending policy in an SPF record in the domain's DNS zone. For example, which email servers they use to send email message from their domain.

When an email server receives a message claiming to come from that domain, the receiving server verifies whether the message complies with the domain's stated policy or not. If, for example, the message comes from an unknown server, it can be considered as fake.

For more information about SPF, refer to About Sender Policy Framework (SPF).

- Enable SPF checking in Hosted Email Security and create the SPF txt record for your domain if you are using Hosted Email Security outbound relay.
    a) Log on to the administrator console.
    b) Go to **Inbound Protection > Domain-based Authentication > Sender Policy Framework (SPF)**
    c) Select the **Enable SPF** check box.
    d) Optionally, enable the option "**Insert X-Header into email messages**"



Inbound Protection › Domain-based Authentication › Sender Policy Framework (SPF)
Add Ignored Peer
Delete

Managed domain: all my domains ▾

☑ Enable SPF

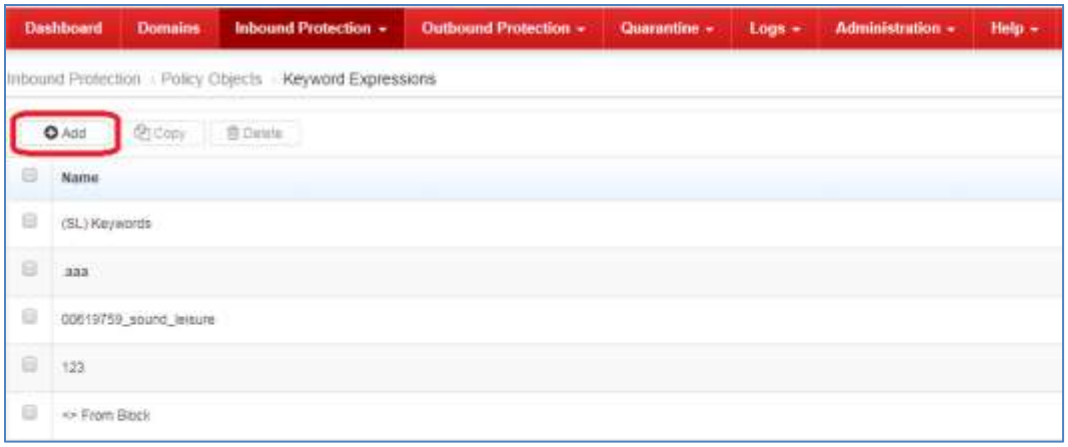
☑ Insert an X-Header into email messages

- Create a policy to track email messages tagged by Hosted Email Security SPF check due to SoftFail.

See Enabling or Disabling Sender Policy Framework (SPF) for the list of SPF results.

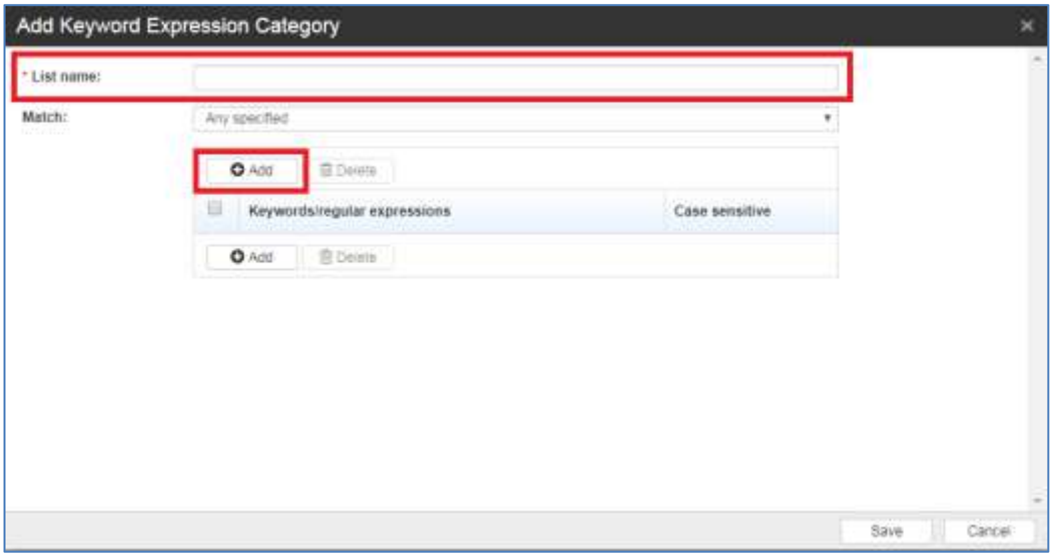
NOTE: Emails that fail the SPF checking due to hard fail will already be blocked and logged by Hosted Email Security. So there is no need to create an additional policy to track them.

a) Log on to the administrator console.
b) Go to **Inbound Protection > Policy Objects > Keyword Expressions** and click **Add.**



	Name
□	(SL) Keywords
□	aaa
□	00619759_sound_leisure
□	123
□	<> From Block

c) Type a name for the keyword list (Ex. SPF Soft Fail). Then click on **Add**.

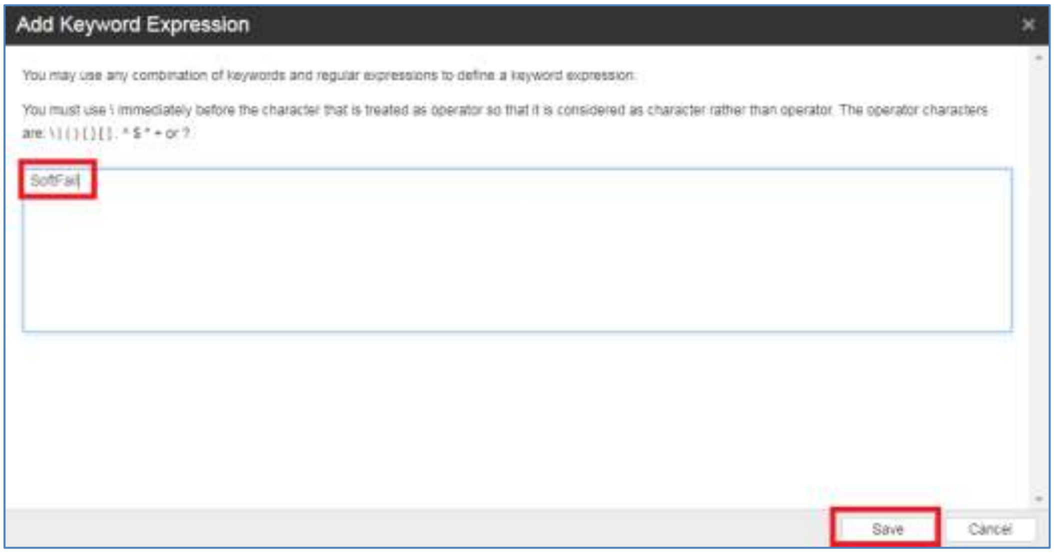


Add Keyword Expression Category

* List name:

Match: Any specified

d) On the **Add Keyword Expression** page, type ***SoftFail*** then click **Save** twice.



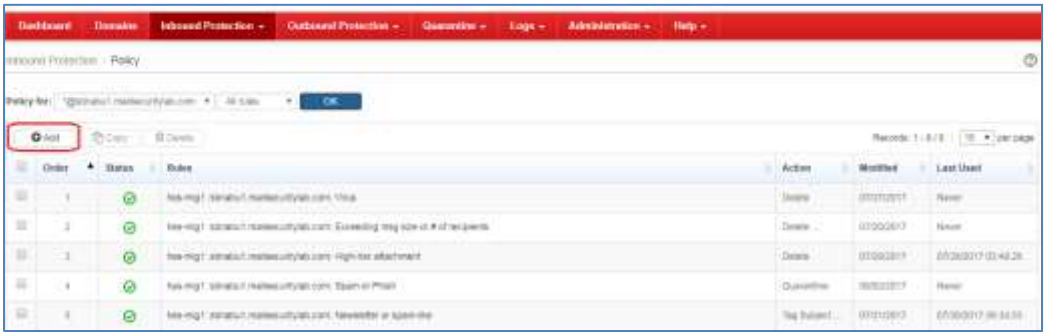
Add Keyword Expression

You may use any combination of keywords and regular expressions to define a keyword expression.

You must use \ immediately before the character that is treated as operator so that it is considered as character rather than operator. The operator characters are: \ | ( ) { } [ ] . ^ $ * + or ?

SoftFail

e) Go to **Inbound Protection > Policy** and click **Add**.

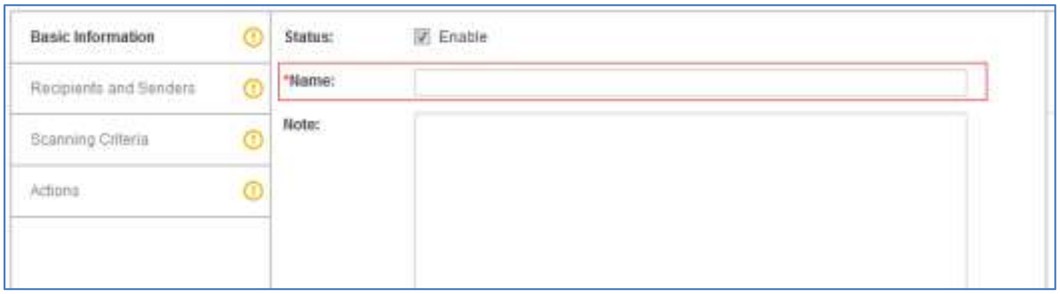


Policy for: *@sbratu1.mailsecuritylab.com | All rules

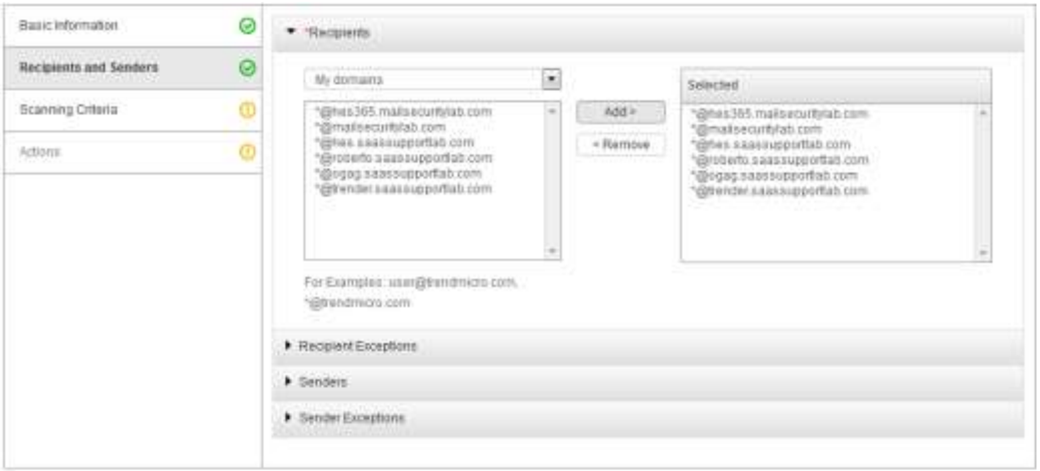
Records: 1 - 8 / 8 | 10 per page

	Order	Status	Rules	Action	Modified	Last Used
□	1	✓	hes-mg1: sbratu1.mailsecuritylab.com: Virus	Delete	[illegible]	Never
□	2	✓	hes-mg1: sbratu1.mailsecuritylab.com: Exceeding msg size or # of recipients	Delete ...	[illegible]	Never
□	3	✓	hes-mg1: sbratu1.mailsecuritylab.com: High-risk attachment	Delete	[illegible]	[illegible]
□	4	✓	hes-mg1: sbratu1.mailsecuritylab.com: Spam or Phish	Quarantine	[illegible]	Never
□	5	✓	hes-mg1: sbratu1.mailsecuritylab.com: Newsletter or spam-like	Tag Subject...	[illegible]	[illegible]

f) Under **Basic Information**, check then **Enable** box then type the name of your policy (Ex. SPF check).



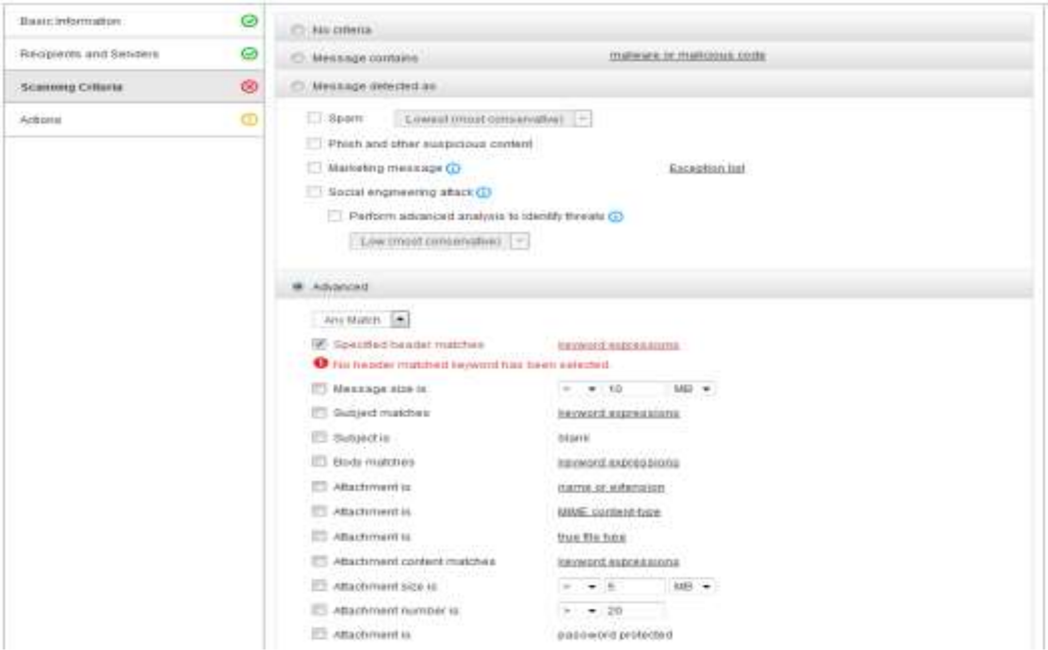
g) Under **Recipients and Senders**, in the **Recipients** section, add all your domains.



*@hes365.mailsecuritylab.com
*@mailsecuritylab.com
*@hes.saassupportlab.com
*@roberto.saassupportlab.com
*@ogag.saassupportlab.com
*@trender.saassupportlab.com

For Examples: user@trendmicro.com, *@trendmicro.com

h) Under **Scanning Criteria**, select **Advanced** and check **Specified header matches**.



Basic Information
Recipients and Senders
Scanning Criteria
Actions

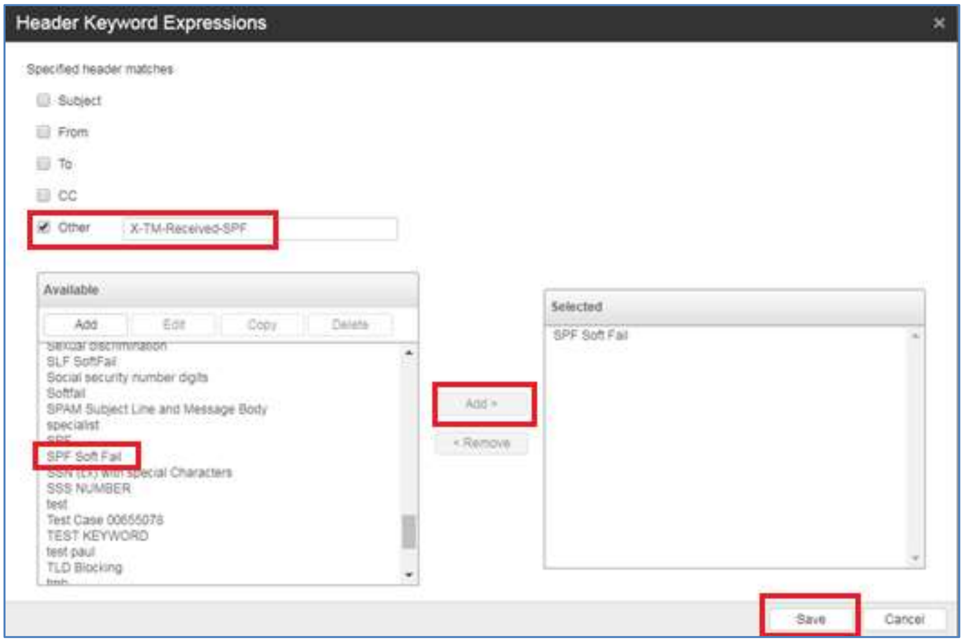
○ No criteria
○ Message contains — malware or malicious code
○ Message detected as
- □ Spam — Lowest (most conservative)
- □ Phish and other suspicious content
- □ Marketing message — Exception list
- □ Social engineering attack
  - □ Perform advanced analysis to identify threats — Low (most conservative)

● Advanced

Any Match

- ☑ Specified header matches — keyword expressions
- No header matched keyword has been selected
- □ Message size is — > 10 MB
- □ Subject matches — keyword expressions
- □ Subject is — blank
- □ Body matches — keyword expressions
- □ Attachment is — name or extension
- □ Attachment is — MIME content-type
- □ Attachment is — true file type
- □ Attachment content matches — keyword expressions
- □ Attachment size is — > 5 MB
- □ Attachment number is — > 20
- □ Attachment is — password protected

i) Click **Keyword expressions** beside **Specified header matches**.
Check **Other** and type the keyword "***X-TM-Received-SPF***".
From the list of **Available** keyword lists, find the list that you created previously. Select it then click on the **Add>** button to move it to the **Selected** list.
Click **Save**.



Header Keyword Expressions

Specified header matches

- □ Subject
- □ From
- □ To
- □ CC
- ☑ Other — X-TM-Received-SPF

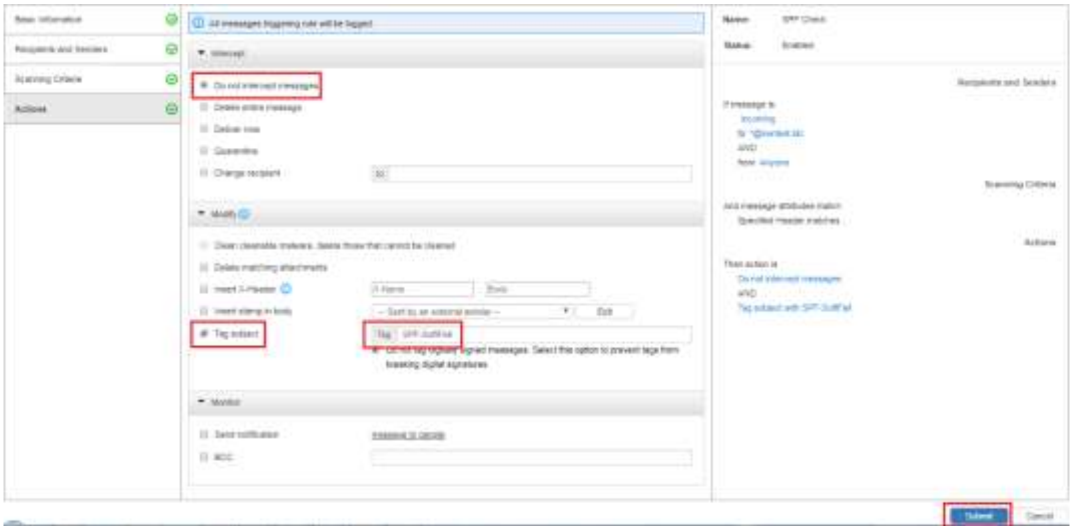
Available

Sexual discrimination
SLF SoftFail
Social security number digits
Softfail
SPAM Subject Line and Message Body
specialist
SPF
SPF Soft Fail
SSN (EX) with special Characters
SSS NUMBER
test
Test Case 00655078
TEST KEYWORD
test paul
TLD Blocking

Selected

SPF Soft Fail

j) Under **Actions**, select your desired action. If your goal is only to log or track emails with SoftFail SPF result, select **Do not intercept messages**. Optionally, you may enable the **Tag subject** action and type the tag that you want to use.



k) Click **Submit.**

3.3.5 Enable DKIM Signature Checking

DomainKeys Identified Mail (DKIM) is an email validation system that detects email spoofing by validating a domain name identity associated with a message through cryptographic authentication. In addition, DKIM is used to ensure the integrity of incoming messages or ensure that a message has not been tampered with in transit.

By enabling DKIM Verification, Hosted Email Security can check the DKIM signatures on incoming email messages and ensure that they come from the domains/senders they claim to be. In addition, the administrator can identify "Enforced Peers", which is a list of domains that must have DKIM signatures on their mails. Actions taken are configurable for email messages that do not pass the DKIM checking.

For more information about DKIM in Hosted Email Security, refer to About DomainKeys Identified Mail (DKIM).

To configure DKIM Signature Verification:

a) Go to **Inbound Protection > Domain-based Authentication > DomainKeys Identified Mail (DKIM) Verification**.

b) Click **Add**. The **Add DKIM Verification Settings** screen appears.

c) Select a specific recipient domain from **the Domain name** drop-down list.

d) Select **Enable DKIM verification**.

e) Optionally select **Insert an X-Header** into email messages.

X-Header is added to indicate whether DKIM verification is successful or not.

Here are some examples of X-Header:

X-TM-Authentication-Results:dkim=pass; No signatures and verification is not enforced
X-TM-Authentication-Results:dkim=pass; No valid signatures and verification is not enforced
X-TM-Authentication-Results:dkim=fail; No processed signatures but verification is enforced
X-TM-Authentication-Results:dkim=pass; Contain verified signature, header.d=test.com, header.s=TM-DKIM_201603291435, header.i=sender@test.com X-TM-Authentication-Results:dkim=fail; No verified signatures

f) Under **Intercept**, select an action that you want to take on a message that fails DKIM verification.

- Do not intercept messages
- Delete entire message
- Quarantine

g) Under **Tag and Notify**, select further actions that you want to take on the message.

- Tag subject

Note:

*Tags can be customized. When selecting the **Tag subject** action, note the following:*

- *This action may destroy the existing DKIM signatures in email messages, leading to a DKIM verification failure by the downstream mail server.*
- *To prevent tags from breaking digital signatures, select **Do not tag digitally signed messages**.*

- Send notification

h) Under **Enforced Peers**, add enforced peers to enforce DKIM verification for specific sender domains.

a. Click **Add**.

b. Specify a sender domain name and click **Add**.

All email messages from the specified domain must pass verification according to the DKIM standard; otherwise, messages will be taken action.

i) Click **Add** to finish adding the DKIM verification settings.

3.3.6 Enable DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email validation system designed to detect and prevent email spoofing. It is intended to combat certain techniques often used in phishing and email spam, such as email messages with forged sender addresses that appear to originate from legitimate organizations. It provides a way to authenticate email messages for specific domains, send feedback to senders, and conform to a published policy.

DMARC is designed to fit into the existing inbound email authentication process of Hosted Email Security. The way it works, is to help email recipients to determine if the purported message aligns with what the recipient knows about the sender. If not, DMARC includes guidance on how to handle the non-aligned messages

To enable DMRAC:

1. Log on to the administrator console.

2. Go to **Inbound Protection > Domain-based Authentication > Domain-based Message Authentication, Reporting and Conformance (DMARC)**

3. Click on the red X under the **Status** column to enable DMARC for all domains, or click **Add** to enable DMARC check for a specific domain.

For details about the different settings available in DMARC, refer to the Adding DMARC Settings section in the Administrator's Guide.

3.3.7 Approved and Blocked Senders

Take extra care in using the Approved and Blocked Senders feature. Ensure that you are adding only what is necessary and consider any possible repercussions.

3.3.7.1 Approved Senders

a. Minimize the amount of addresses in the **Inbound Protection > Sender Filter > Approved Senders** list. Addresses in the Approved Senders bypass all anti-spam, spoofed email message, and IP Reputation checks.
b. Do not put an internal email address or domain in the Approved Senders list.

3.3.7.2 Blocked Senders

a) Only add addresses that are confirmed to be spammers or sending unwanted or malicious email messages.

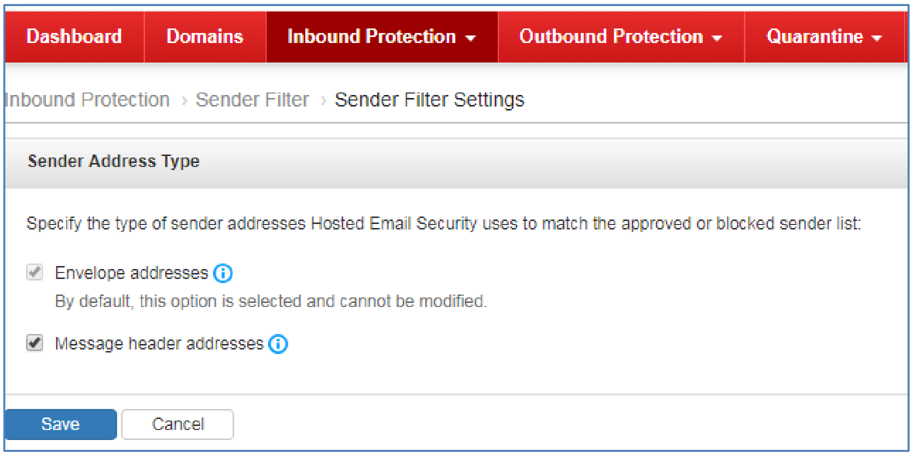
b) If no internal email message passes through Hosted Email Security, internal domains may be added in the Blocked Senders list to protect against envelope sender spoofing.

c) Limit the amount of entries to a manageable number.

3.3.7.3 Sender Filter Settings

The sender filter settings provide an option for the administrator to specify which sender addresses will be checked against the list of approved and blocked senders. The setting can be accessed from Administrator Console > Inbound Protection > Sender Filter > Sender Filter Settings.

Options include using Envelope addresses, Message header addresses, or both.



Inbound Protection › Sender Filter › Sender Filter Settings

Sender Address Type

Specify the type of sender addresses Hosted Email Security uses to match the approved or blocked sender list:

☑ Envelope addresses ⓘ
By default, this option is selected and cannot be modified.

☑ Message header addresses ⓘ

For more details, refer to this Knowledge Base article.

3.4 Backscatter spam and Directory Harvest Attacks (DHA) Email Messages

Hosted Email Security uses user directories to help prevent backscatter (or outscatter) spam and Directory Harvest Attacks (DHA). Importing user directories lets Hosted Email Security know legitimate email addresses and domains in your organization.

Enable Directory management to prevent these types of malicious email messages. Directory Management can be done in two ways:

- Importing User Directories
- Synchronizing User Directory from LDAP

See About Directory Management

Once user directories are imported or synced to Hosted Email Security, enable Recipient Filter for the domain.

a) Go to **Inbound Protection** > **Recipient Filter**.

b) Look for your domain on the list.

c) Click the icon under **Status** column to toggle it from Disabled (Red X) to Enabled (Check) and vice versa.

3.5 Incoming Transport Layer Security (TLS)

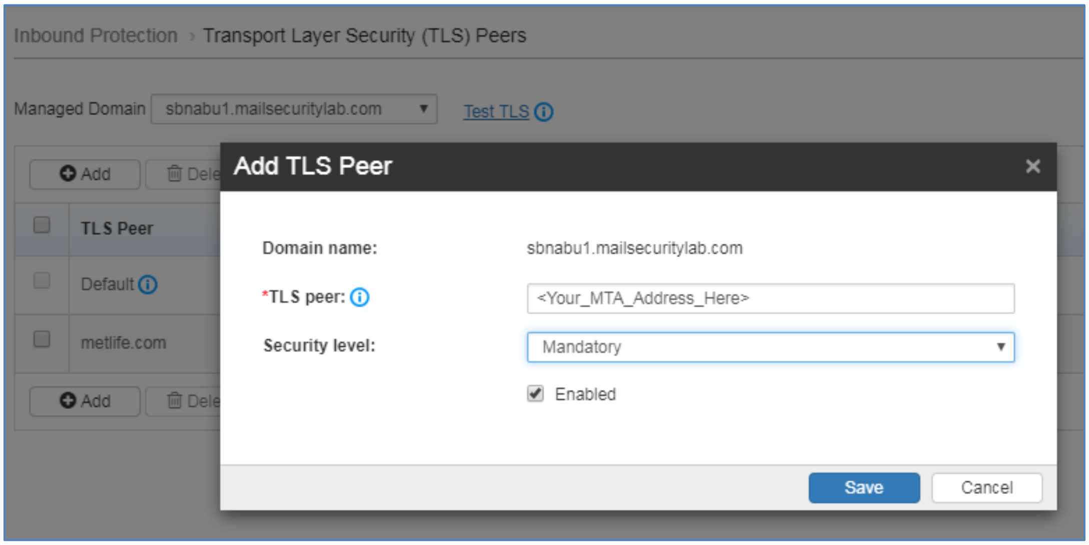
Transport Layer Security (TLS) is a protocol that helps to secure data and ensure communication privacy between endpoints. Hosted Email Security allows you to configure TLS encryption policies between Hosted Email Security and specified TLS peers. Hosted Email Security supports the following TLS protocols in descending order of priority: TLS 1.2, TLS 1.1, and TLS 1.0.

Under **Inbound Protection > Transport Layer Security (TLS) Peers** of the administrator console, Hosted Email Security has a Default policy that enables Opportunistic TLS on all inbound communications. This includes connections from hosts or MTA's in the Internet for incoming email messages, and connections from customer's MTAs for outgoing email messages.

Certain organizations and businesses such as medical, banking, or government organizations may have compliance requirements and require TLS on all communications. In such cases, you may configure Hosted Email Security to force TLS when communicating with those domains.

For a stricter implementation, add the domains, IP addresses and IP blocks that you trust to use TLS in all its communication.

1. From Hosted Email Security administrator's console, go to **Inbound Protection > Transport Layer Security (TLS) Peers**.
2. Select your domain from the **Managed Domain** drop-down list.
3. Click **Add**.
4. Type the address of your own or partner MTA that must use TLS in all its communication.
5. Select **Security Level** as **Mandatory**.
6. Click **Save**.


Inbound Protection › Transport Layer Security (TLS) Peers

Managed Domain: sbnabu1.mailsecuritylab.com

Add TLS Peer

Domain name: sbnabu1.mailsecuritylab.com

*TLS peer: <Your_MTA_Address_Here>

Security level: Mandatory

☑ Enabled

For more information about TLS settings in Hosted Email Security, refer to About Transport Layer Security (TLS) Peers.

3.6 Ransomware Protection

Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to restore access to their systems, or to get their data back.

Ransomware can be downloaded by unwitting users who visit malicious or compromised websites. It can also arrive as a payload, either dropped or downloaded by other malware. Some ransomware are delivered as attachments to spammed email message.

To increase protection from Ransomware threats in Hosted Email Security:

- Enable IP reputation setting. For the procedure, refer to this KB article: Configuring the IP Reputation settings to block spam on Hosted Email Security (HES).
- Make sure Spam and Phish inbound policy is enabled. This includes WRS, new born URL handling and TLSH. Follow the instructions on Troubleshooting guide for spam mails not filtered by Hosted Email Security (HES).
- Block file types commonly used by Ransomware. To do this, refer to this KB article: Blocking attachments using the Attachment True File Type criteria in Hosted Email Security (HES).

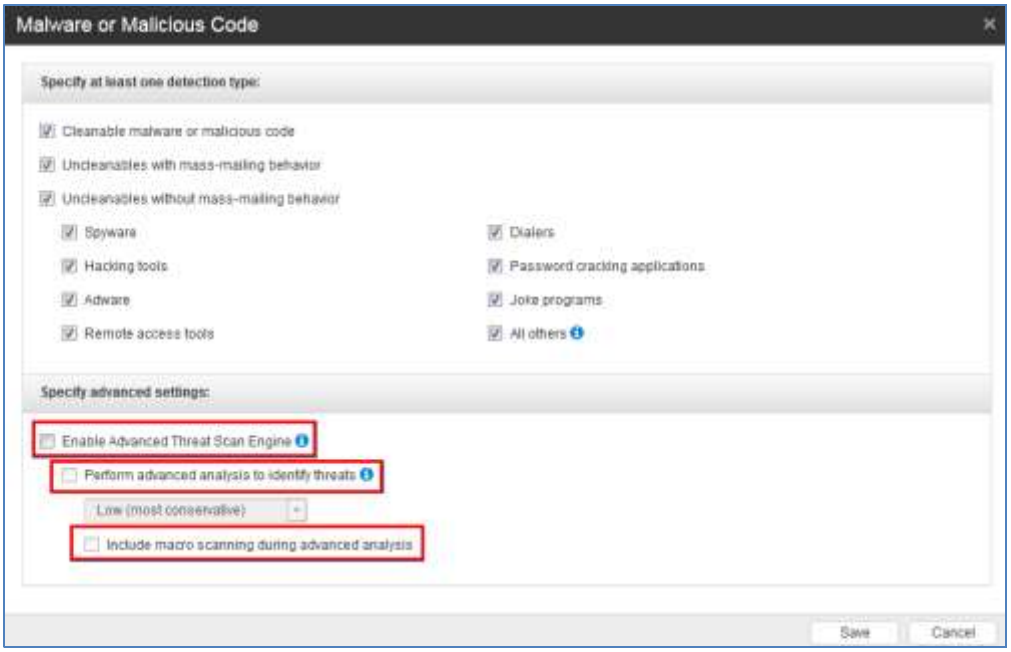
- Enable macro file scanning.

Hosted Email Security now supports Deep Discovery Analyzer as a Service (DDAaaS), which is a cloud-based web service that acts as an external analyzer.

Enabling this feature will help detect macro embedded files. It identifies suspicious files, sends them to the sandbox, and then takes an action.

To integrate Hosted Email Security with DDAaaS:

1. Log on to Hosted Email Security Administrator console.
2. Go to **Inbound Protection** > **Policy** and select **Virus Rule**.
3. Go to **Scanning Criteria** > **Malware or Malicious Code**.
4. Under **Specify advanced settings**, select **Enable Advance Threat Scan Engine** and **Perform advanced analysis to identify threats**. Then select **Include macro scanning during advanced analysis**.



Malware or Malicious Code

Specify at least one detection type:

☑ Cleanable malware or malicious code
☑ Uncleanables with mass-mailing behavior
☑ Uncleanables without mass-mailing behavior

☑ Spyware	☑ Dialers
☑ Hacking tools	☑ Password cracking applications
☑ Adware	☑ Joke programs
☑ Remote access tools	☑ All others

Specify advanced settings:

□ Enable Advanced Threat Scan Engine
□ Perform advanced analysis to identify threats
Low (most conservative)
□ Include macro scanning during advanced analysis

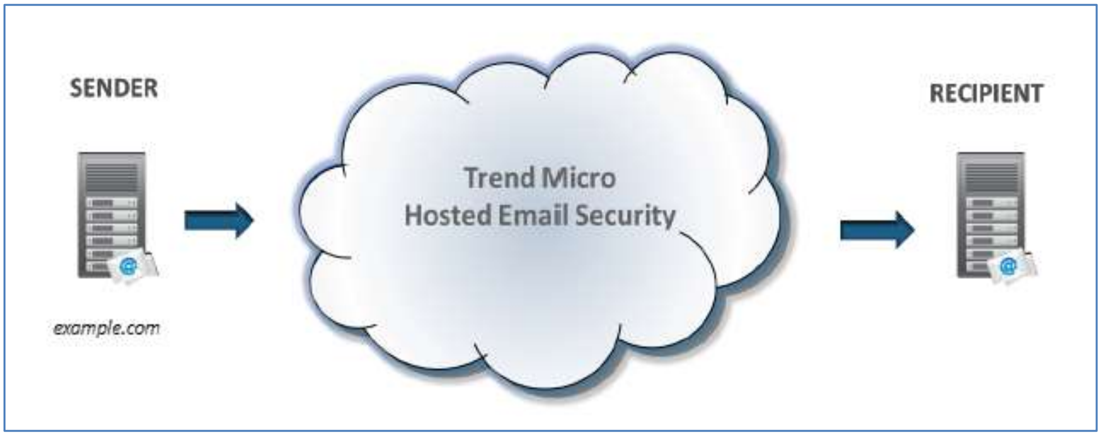
5. Click **Save**.

Hosted Email Security can perform advanced analysis on samples in a closed environment to identify suspicious objects that traditional scanning may not detect. When enabled, Hosted Email Security delays the delivery of the messages until the advanced analysis completes, which may take up to 30 minutes.

4 Outbound Mail Protection

4.1 Using Outbound Filtering

When using Hosted Email Security for filtering outbound mails, email traffic will be configured as described below.



1. Mail server of example.com will forward the outbound email message to Hosted Email Security.
2. Hosted Email Security servers accept the message and performs message filtering and policy matching on your behalf.
3. Assuming that the message is slated for delivery according to its security policy or validity status, the email message will be forwarded to outbound MTAs.
4. Outbound MTAs will then route this email message to the mail server of the recipient.

4.2 Policies

Hosted Email Security has separate policies applied to outbound email messages. Depending on each organization's needs, these policies may be adjusted to meet specific requirements.

4.2.1 Outbound-Virus Policy

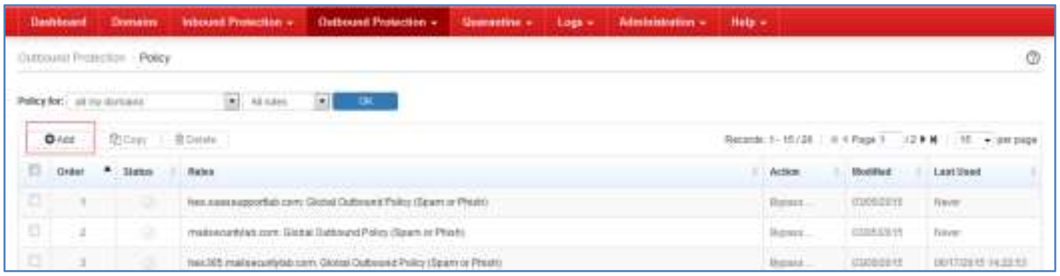
By default, Hosted Email Security has an Outbound – Virus policy enabled. This policy scans for possible malicious files that may come from your network. Make sure to keep this policy enabled to protect your organization from possible damage reputation due to malware spread.

4.2.2 Add additional outbound spam and phish policy

Hosted Email Security Global Outbound Policy is a default rule in Hosted Email Security to avoid outbound spam and prevent Hosted Email Security outbound servers from being blacklisted by third-party Real-time Blackhole Lists (RBLs). The policy cannot be edited and they are activated by default for all domains. Default action for this policy is “do not intercept” and email messages filtered by this policy will be sent to a special server to deliver.

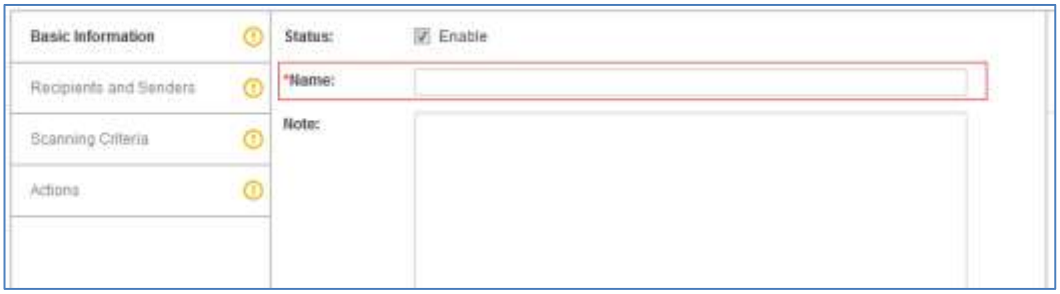
To control your outbound spam and phish email messages, it is recommended to create a new outbound spam and phish policy.

1. Log on to the Hosted Email Security Administrator console.
2. Go to **Outbound Protection > Policy** and click **Add**.



Order	Status	Rules	Action	Modified	Last Used
1		hes.saassupportlab.com: Global Outbound Policy (Spam or Phish)	Bypass ...	[illegible]	Never
2		mailsecuritylab.com: Global Outbound Policy (Spam or Phish)	Bypass ...	[illegible]	Never
3		hes365.mailsecuritylab.com: Global Outbound Policy (Spam or Phish)	Bypass ...	[illegible]	[illegible]

3. Under **Basic Information**, type the name of your policy.

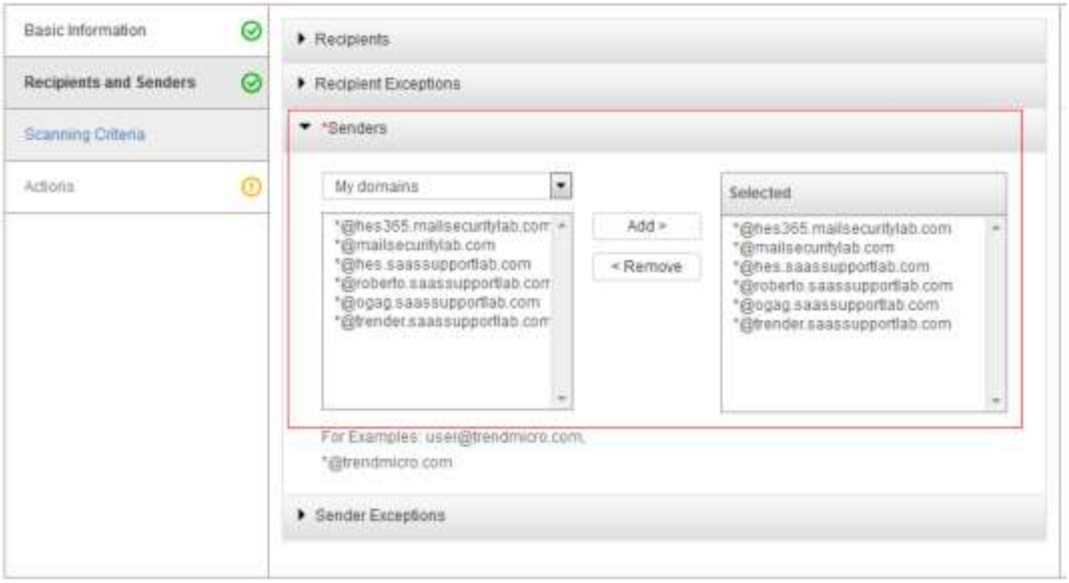


Status: ☑ Enable

*Name:

Note:

4. Under **Recipient and Sender**, in the **Senders** field, expand senders and add all your domains.


Basic Information
Recipients and Senders
Scanning Criteria
Actions

▸ Recipients
▸ Recipient Exceptions
▾ *Senders

My domains
*@hes365.mailsecuritylab.com
*@mailsecuritylab.com
*@hes.saassupportlab.com
*@roberto.saassupportlab.com
*@ogag.saassupportlab.com
*@trender.saassupportlab.com

Add >
< Remove

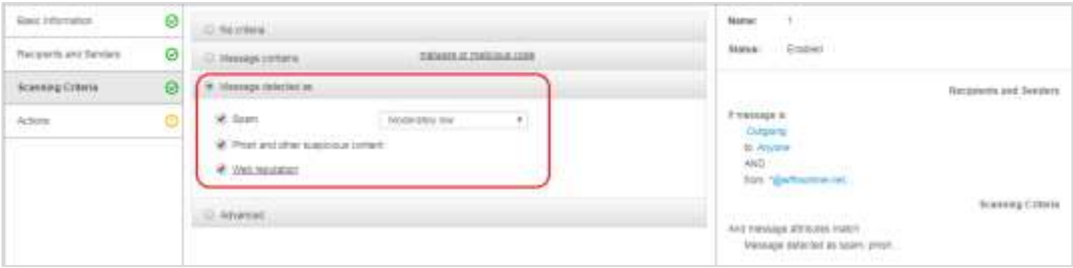
Selected
*@hes365.mailsecuritylab.com
*@mailsecuritylab.com
*@hes.saassupportlab.com
*@roberto.saassupportlab.com
*@ogag.saassupportlab.com
*@trender.saassupportlab.com

For Examples: user@trendmicro.com,
*@trendmicro.com

▸ Sender Exceptions

.

5. Under **Scanning Criteria**, select **Message Detected as** and check all boxes. You can adjust the detection level based on your needs. Note that setting spam check higher might lead to more false positive but it can also reduce false negative email messages and avoid malicious email messages.


Basic Information
Recipients and Senders
Scanning Criteria
Actions

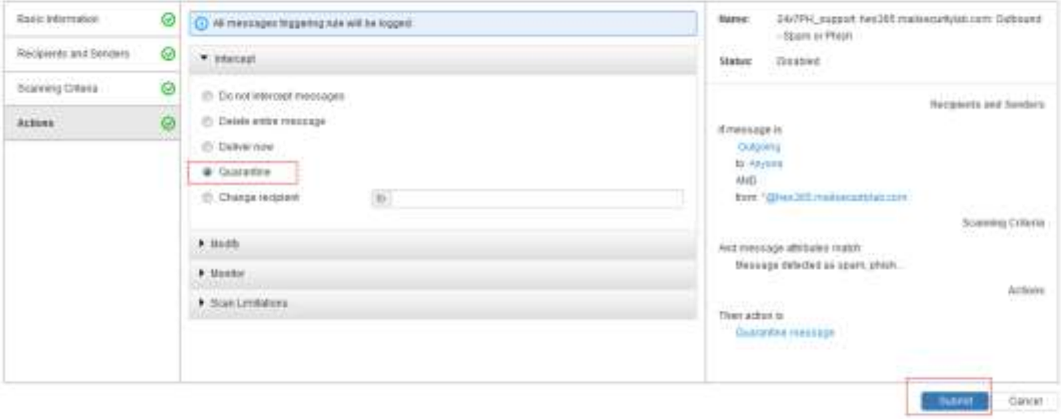
○ No criteria
○ Message contains [illegible]
● Message detected as
☑ Spam: Moderately low
☑ Phish and other suspicious content
☑ Web reputation
○ Advanced

Name: 1
Status: Enabled

Recipients and Senders
If message is
Outgoing
to: Anyone
AND
from: *@[illegible].net

Scanning Criteria
And message attributes match
Message detected as spam, phish...

6. Under **Actions**, select your desired action such as “quarantine” and click **Submit**.


Basic Information
Recipients and Senders
Scanning Criteria
Actions

All messages triggering rule will be logged
▾ Intercept
○ Do not intercept messages
○ Delete entire message
○ Deliver now
● Quarantine
○ Change recipient
▸ Modify
▸ Monitor
▸ Scan Limitations

Name: 24/7PH_support hes365.mailsecuritylab.com: Outbound - Spam or Phish
Status: Disabled

Recipients and Senders
If message is
Outgoing
to: Anyone
AND
from: *@hes365.mailsecuritylab.com

Scanning Criteria
And message attributes match
Message detected as spam, phish...

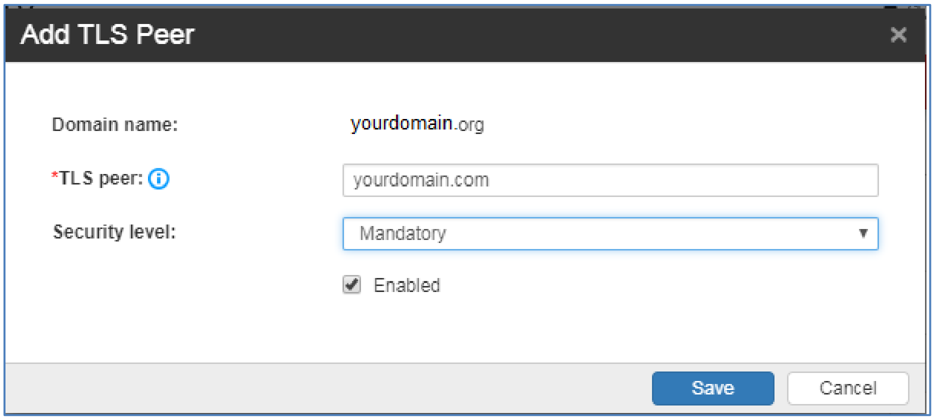
Actions
Then action is
Quarantine message

Submit
Cancel

4.3 Outgoing TLS

Similar to Incoming TLS, Hosted Email Security also has a default policy that enables Opportunistic TLS for all outgoing connections. This includes connections from Hosted Email Security to email messages going to the Internet or to customer's own mail server or MTA. For a more secure connection, create TLS Peers setting for recipient domains that you trust, including your own. Hosted Email Security will use TLS when sending email messages to these domains.

a) From Hosted Email Security administrator console, go to **Outbound Protection** > **Transport Layer Security (TLS) Peers**.
b) Click **Add**.
c) Type the domain name in the **TLS Peer** text box.
d) Select the mandatory security level.
e) Click **Save**.



Add TLS Peer

Domain name: yourdomain.org

*TLS peer: yourdomain.com

Security level: Mandatory

☑ Enabled

4.4 Publish SPF record in DNS

When using Outbound Filtering in Hosted Email Security, your outbound mails will be routed to Hosted Email Security first. The Hosted Email Security will relay it to the destination domains. Given this, you can add Hosted Email Security outbound IP addresses in your domain's SPF record to let recipients know that your outbound mails should only come from Hosted Email Security.

When using Hosted Email Security outbound scanning, the following is the recommended SPF record:

v=spf1 include:spf.hes.trendmicro.com –all

You may add additional record depending on your environment.

Doing this can prevent malicious attacks from using your domain as the sender address in their spoofed email messages.

4.5 DKIM Signing

By enabling DKIM Signing for outgoing mails, you give the receiving domain the necessary tool to verify all email messages that claim to be coming from your own domain. This prevents attackers from using your domain as the sender in their spoofed email messages.

Enabling DKIM signing is highly recommended when using Hosted Email Security outbound filtering. To enable this:

a) Go to **Outbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Signing**.

b) Click **Add**.

   The **Add DKIM Signing Settings** screen appears.

c) Select a specific sender domain from the **Domain name** drop-down list.

d) Select **Enable DKIM signing**.

e) Configure general settings for DKIM signing.

   - **SDID**: select a signing domain identifier from the drop-down list.
   - **Selector**: selector to subdivide key namespace. Retain the default value.
   - **Headers to sign**: select one or multiple headers to sign and customize more headers if necessary.
   - **Wait time**: specify how long it takes for a key pair to take effect. Hosted Email Security starts to count the wait time once if finds the public key in the DNS.
   - **Key pair**: click **Generate** to generate a key pair.

Note:
*Use the generated **DNS TXT record name** and **DNS TXT record value** to publish the key pair to your DNS server.*
If your domain provider supports the 2048-bit domain key length but limits the size of the TXT record value to 255 characters, split the key into multiple quoted text strings and paste them together in the TXT record value field.

Below is a key pair example:

DNS TXT record name:
TM-DKIM-2017052414923._domainkey.testdomain.com

DNS TXT record value:
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5mHBjC/WCkQ5WRWJ4Ln64EssFPQojX
0yNIOTgjrchcK0/lKX1eRvZzbX8kErmgT5hvEys9tDoW7iG/zAZUqhmtgDuha8ULFknxsvrMhPsVs3jSjX3
73bBWtOgI+izFCH+MU6KznyJZGcckEsPkS3ffyKrOZQAMpv6zu28tx2P8mPMnCqzjxMmPXiBZTJ19/M
kWAU1VHD39bUVByu0dlmQdEodBqcPxyev/pBh++kNpvIpuBnnaXtZCKAYBtqt8HF6w/eimyStcPYtHp
mBY43stCTg5Kr3ON1KRuCN3o/vLUKGPgCPLyjLVh5beme1BRouyxU42s8OLuBEcU9umpKhQIDAQAB

The above TXT record value is one long line of 410 characters. Since some DNS servers accept only up to 255 characters value per record, the above string may be divided into 2 parts. It can be split *at any point as long as each of the divided parts does not exceed 255 characters. Then create 2 TXT records with the same name, each having one part of the divided string. For example:*

TM-DKIM-2017052414923._domainkey	*IN*	*TXT*	*“v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5mHBjC/WCkQ5WRWJ4Ln64EssFPQojX0yNIOTgjrchcK0/lKX1eRvZzbX8kErmgT5hvEys9tDoW7iG/zAZUqhmtgDuha8ULFknxsvrMhPsVs3jSjX373bBWtOgI+izFCH+MU6KznyJZGcckEsPkS3ffy”*
TM-DKIM-2017052414923._domainkey	*IN*	*TXT*	*“KrOZQAMpv6zu28tx2P8mPMnCqzjxMmPXiBZTJ19/MkWAU1VHD39bUVByu0dlmQdEodBqcPxyev/pBh++kNpvIpuBnnaXtZCKAYBtqt8HF6w/eimyStcPYtHpmBY43stCTg5Kr3ON1KRuCN3o/vLUKGPgCPLyjLVh5beme1BRouyxU42s8OLuBEcU9umpKhQIDAQAB”*

f) Configure advanced settings for DKIM signing.

- **Header canonicalization**: select **Simple** or **Relaxed**.
- **Body canonicalization**: select **Simple** or **Relaxed**.

Note:
Two canonicalization algorithms are defined for each of the email header and the email body: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping.

- **Signature expiration**: set the number of days that the signature will be valid.
- **Body length**: set the number of bytes allowed for the email body.
- **AUID**: specify the Agent or User Identifier on behalf of which SDID is taking responsibility.

g) Click **Add** to finish adding the DKIM signing settings.

4.6 Email Encryption

Hosted Email Security can encrypt your outgoing email messages for added security. By using encryption, you protect the email message from eavesdropping and man-in-the-middle attacks. Hosted Email Security does not automatically encrypt email messages. When outbound filtering is enabled, outbound encryption appears as a rule option within the Hosted Email Security administrator console. You will need to configure rules that apply encryption as a rule action.

Special rules can be created so that Hosted Email Security only encrypts email messages between selected people. To use email encryption:

a) From Hosted Email Security administrator’s console, go to **Outbound Protection > Policy.**

b) Click **Add**

c) Type a name for the policy.

d) Under **Recipients and Senders**, specify the senders and recipient addresses of email messages that should be encrypted. Optionally, exceptions can be specified.

NOTE: Both the sender and recipient addresses must match the policy setting for the email to be encrypted. If only the sender or only the recipient is matched, the policy will not apply.

e) Under **Scanning Criteria**, identify the criteria for email messages that should be encrypted. If all mails that match the Sender and Recipient should be encrypted, select **No Criteria**.

f) Under Actions, select **Do not intercept messages** and **Encrypt email** actions.

g) Click **Submit**.

Recipients of the encrypted email message can read the mails either by using Trend Micro Email Encryption Client or using a browser. For more details, refer to Reading an Encrypted Email Message.

5 Other Features and Settings

5.1 Dashboard

After logging in to Hosted Email Security administration console, you will be directed to the dashboard. The dashboard offers a detailed overview about the amount and type of email traffic going to and coming from your network.

Incoming email statistics such as Top Spam Chart, Top BEC Threats, Top Malware Threats, and Top Advanced Analyzed Threats can provide the administrator vital information that may indicate if the organization is under attack. Outgoing statistics, on the other hand, like top senders of malware or spam mail can help identify compromised accounts within the organization.

Regular visit and checking of the dashboard graphs in Hosted Email Security is highly recommended.

5.2 Approved and Blocked Senders

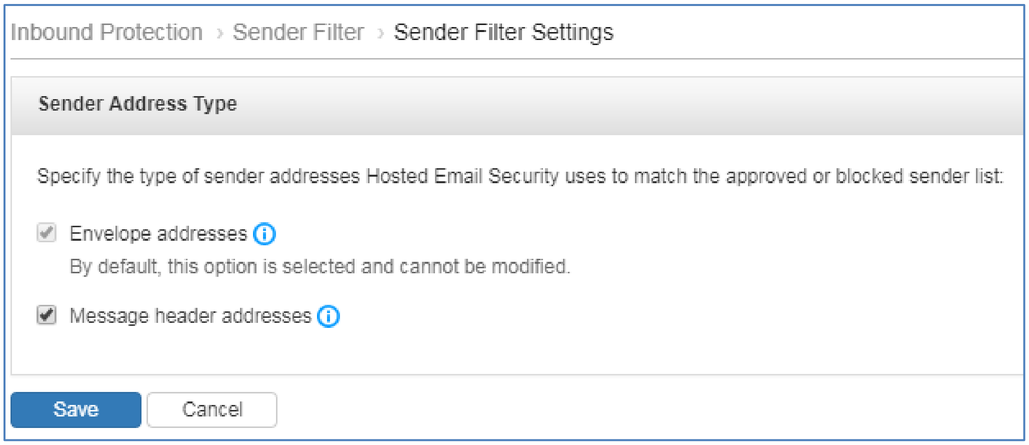
Approved and Blocked Senders Lists are used to bypass some of the filtering criteria in Hosted Email Security. Once matched, the email message is either blocked immediately or skips going through some of the filters related to spam protection. When using this feature, the administrator should:

a. Minimize the amount of addresses in the **Inbound Protection > Sender Filter > Approved Senders** and **Blocked Senders** lists for easier management as well as avoiding possible unintended mail blocking.
b. Addresses in the Approved Senders bypass all spam, spoofed email message, and IP Reputation checks. So make sure to put only trusted addresses here.
c. Never put an internal email address or domain in the Approved Senders list to avoid spoofed email attacks.

5.3 Sender Filter Settings

Configure Hosted Email Security to check both Envelope Header Sender and Message Header Sender addresses for matching Approved and Blocked senders.

a) From the Hosted Email Security administration console, go to **Inbound Protection > Sender Filter > Sender Filter Settings**.
b) Enable the checkbox for **Message header addresses**.
c) Click **Save**.


Inbound Protection › Sender Filter › Sender Filter Settings

Sender Address Type

Specify the type of sender addresses Hosted Email Security uses to match the approved or blocked sender list:

☑ Envelope addresses

By default, this option is selected and cannot be modified.

☑ Message header addresses

In addition to matching Approved and Blocked Senders in both the Administrator defined list and End-User Quarantine (EUQ), this also affects the way Hosted Email Security sends and shows that list of email messages in users' EUQ console.

For details, refer to Sender Filter feature enhancement in Hosted Email Security.

5.4 Regular Expressions

Regular expressions, often called regex, are sets of symbols and syntactic elements used to match patterns of text. Hosted Email Security can use regular expression (regex) to filter out keywords in the email message.

Using long and complex regular expression are more prone to errors and false detection so it's recommended to split long and complex keyword expression to several entries.

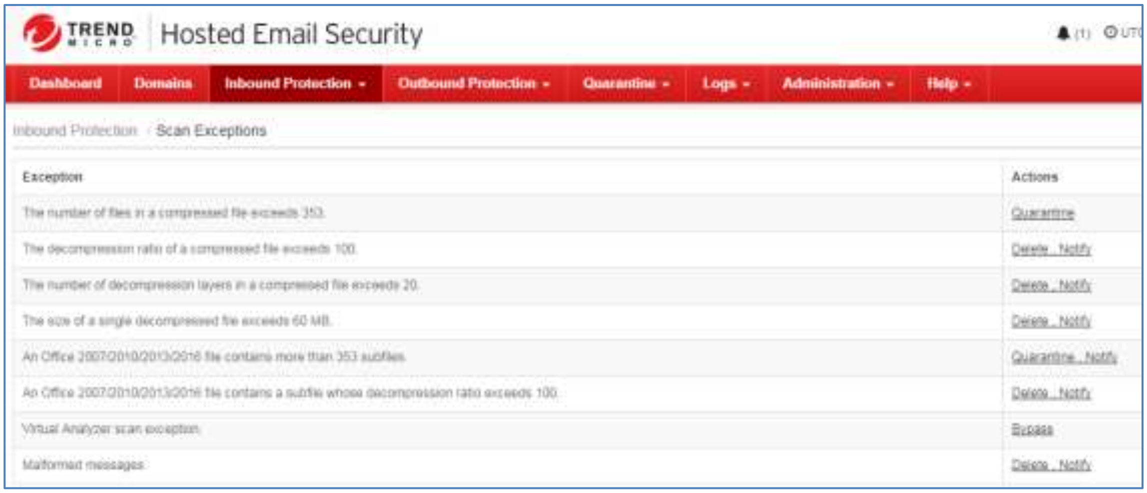
Also, limit the use of wildcards especially asterisk (*). The use of multiple asterisks in a single regex makes it prone to false positive detections.

See About Keyword Expressions

5.5 Scan Exceptions

Under certain circumstances, you may want to prevent Hosted Email Security from scanning certain types of messages that may pose security risks. For example, compressed files provide a number of special security concerns since they can harbor security risks or contain numerous compression layers.

Scan Exceptions setting in Hosted Email Security is found under **Inbound Protection** > **Scan Exceptions** and **Outbound Protection** > **Scan Exceptions**.



Inbound Protection / Scan Exceptions

Exception	Actions
The number of files in a compressed file exceeds 353.	Quarantine
The decompression ratio of a compressed file exceeds 100.	Delete , Notify
The number of decompression layers in a compressed file exceeds 20.	Delete , Notify
The size of a single decompressed file exceeds 60 MB.	Delete , Notify
An Office 2007/2010/2013/2016 file contains more than 353 subfiles.	Quarantine , Notify
An Office 2007/2010/2013/2016 file contains a subfile whose decompression ratio exceeds 100.	Delete , Notify
Virtual Analyzer scan exception.	Bypass
Malformed messages.	Delete , Notify

Sometimes, normal files may trigger the scan exceptions due to the number of files inside a compressed or Office file. When situations like this occur, it is NOT recommended to set the action to Bypass. Doing so creates a risk of malware getting through unscanned. Instead, choose the Quarantine action. If a normal file is quarantined, use the Quarantine Query feature of the administration console to search for the email message, and then choose to deliver it.

5.6 Message Retention and Quarantine Management

The following table shows message retention information:

ITEM	RETENTION
Quarantined Email Messages	30 days
Message Tracking Logs	90 days
Message Queue (when customer MTA is down)	Up to 10 days

Note:
Incoming Message queue is up to 10 days but outgoing queue will only be kept for 1 day.

With the above information, it is necessary to ensure that quarantined messages are properly managed before they get purged. Quarantined messages may be queried and any essential email message that was inadvertently quarantined can be released. To manage quarantined email messages:

1. Log on to the Hosted Email Security Administrator console.
2. In the **Dates** fields, select a range of dates.

Note:
Queries include data for up to seven continuous days in one calendar month. Use more than one query to search across calendar months.

3. In the **Direction** field, select a mail traffic direction.
4. Type your search criteria into one or more of the following fields:
   - **Recipient**
   - **Sender**
   - **Subject**

A recipient or sender can be a specific email address or all addresses from a specific domain.

- Query a specific email address by typing that email address.
- Query all addresses from a domain by using an asterisk (*) to the left of the at sign (@) in the email address. For example, *@example.com will search for all email addresses in the example.com domain.

5. Click **Search**.
6. Select one or multiple messages to manage.
7. Click one of the following buttons to manage the selected messages:
   - **Delete**: Cancel delivery and permanently delete the message
   - **Deliver**: Release from quarantine

> ***Note:***
> *Released messages are no longer marked as spam, but they will continue to be processed by Hosted Email Security. The following conditions apply to delivery:*
> *a) If a message triggers a content-based policy rule with an **Intercept** action of **Quarantine**, it will once again appear in the quarantined message list.*
> *b) If a message triggers a content-based policy rule with an **Intercept** action of **Delete entire message** or **Change recipient**, it will not arrive at its intended destination.*

8. Optionally click on the **Timestamp** value to view the **Quarantine Query Details** screen for a given message.
   a. Check the summary and message view information about the message.
   b. Click **Delete**, **Deliver**, or **Download** to manage the message.

> ***Note:***
>
> ***Download**: Download the message to your local host.*
>
> *This button is available only on the **Quarantine Query Details** screen.*

5.7 Quarantine Digest

To ease the management effort on the part of the administrator, enabling and configuring EUQ Digest mail is a popular option. The Quarantine Digest lists up to 100 of each end user's quarantined email messages, and provides a link for that account holder to access quarantined messages through the End User Quarantine website at the following web address for your region:

- For Europe, the Middle East, Africa: https://euq.hes.trendmicro.eu
- For all other regions: https://euq.hes.trendmicro.com

Use the **Digest Settings** screen to configure the schedule and format for the Quarantine Digest. If the digest is enabled, all domain recipients receive their own customized copy of the digest. Intended message recipients can use the End User Quarantine website to manage messages in quarantine themselves. For details on how to enable and configure EUQ Digest settings, refer to Configuring the Quarantine Digest.

The Quarantine Digest email message features a template with customizable plain-text and HTML versions. Each version of the template can incorporate "tokens" to customize output for digest recipients.

If the **Inline Action** check box is selected on the **Digest Settings** screen, recipients can directly manage their quarantine from the digest email message. By enabling this function, you can relieve users of the necessity of logging on to the End User Quarantine website and manually approving quarantined messages or senders.

Warning: *Anyone receiving this Quarantine Digest email message will be able to add any of these senders to the account holder's approved senders list. Therefore, administrators must warn digest recipients not to forward the Quarantine Digest email message. The Quarantine Digest for managed accounts is sent to the primary account. For more information about managed accounts, see About End-User Managed Accounts.*

5.8 General Order of Evaluation

Hosted Email Security follows a specific order in evaluating email messages. Knowing this order helps a lot in identifying and troubleshooting email blocking concerns. The order is outlined below.

1. Sender email addresses filtering:

   Message sender email addresses and domains go through approved sender and blocked sender list filtering. Sender email addresses are evaluated until the first match is found.

   See Sender Filter Order of Evaluation.

   Messages from allowed sender addresses bypass IP reputation-based filtering at the MTA connection level and content-based filtering at the message level for spam detection, and proceed directly to virus detection. Messages from blocked email addresses are blocked.

2. IP reputation-based filtering at the MTA connection level:

   Message sender IP addresses go through IP reputation-based filtering. IP addresses are evaluated until the first match is found.

   See IP Reputation Order of Evaluation.

   Messages from allowed sender IP addresses bypass IP reputation-based filtering at the MTA connection level and proceed to spam detection. Messages from blocked sender IP addresses are blocked.

3. Domain-level policy filtering:

   Messages will pass each one of the policies for filtering depending on the action on the first triggered policy.

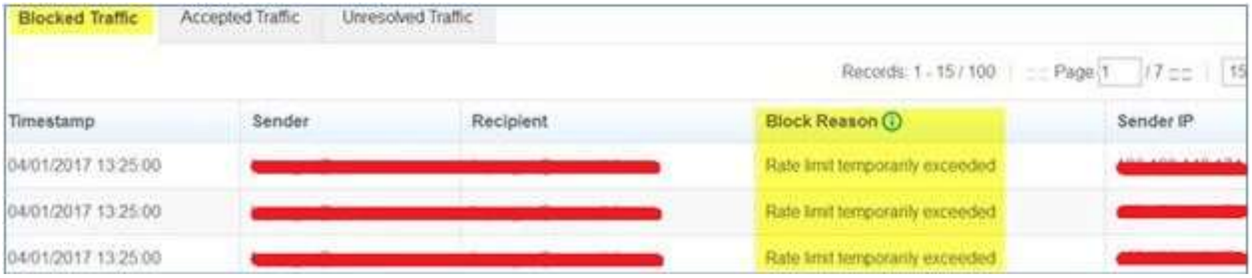
Messages from allowed sender addresses bypass IP reputation-based filtering at the MTA connection level and content-based filtering at the message level for spam detection, and proceed directly to virus detection. Messages from blocked email addresses are blocked.

Note: Hosted Email Security takes action on email messages that pass Email Reputation and custom approved list filtering using the policy rules configured for content-based filters. For example, Hosted Email Security may quarantine an infected email message from an address in the approved senders list if you have configured content-based filtering to quarantine malware threats.

5.9 Bulk Email Sending

Sending bulk email messages through Hosted Email Security is not a supported use case. Hosted Email Security is an email security service that focuses on keeping your email messages secure and free from malicious contents. It is not a Bulk Email Service Provider, a totally different type of email service.

Hosted Email Security is able to identify senders with anomalous outbound email behavior – for example, sending bulk email messages or sudden increase in email volume. Depending on the dynamic threshold settings, Hosted Email Security will take actions like temporarily block email messages for a certain period of time. When this happens, Hosted Email Security Mail Tracking will log the rate limited email messages like the picture below.



Timestamp	Sender	Recipient	Block Reason	Sender IP
04/01/2017 13:25:00	[redacted]	[redacted]	Rate limit temporarily exceeded	[redacted]
04/01/2017 13:25:00	[redacted]	[redacted]	Rate limit temporarily exceeded	[redacted]
04/01/2017 13:25:00	[redacted]	[redacted]	Rate limit temporarily exceeded	[redacted]

This mechanism is Hosted Email Security's way of protecting not just itself but also all our customers from the following situations:

- **Service Abuse** – Without burst email detection, it will be easy for any client to abuse the service with burst email sending. Such abusive behavior may cause service disruption and damage to the service's reputation.
- **3rd Party RBL Listing** – 3rd IP Reputation or Real-Time Blackhole List (RBL) providers may add Hosted Email Security' IP address to their blocked list when burst email behavior is detected from one or more of its outbound MTA. Since Hosted Email Security is a multi-tenant service, multiple customers may be affected if its IP is blocked by 3rd party RBL providers.
- **Denial-of-Service** - Without rate limiting, it may be possible for an attacker to launch a simple Denial-of-Service attack by continuously sending huge amounts of email messages within a short period of time.

When faced with this scenario, customers have the following options if there is a requirement for sending email messages in bulk like newsletters and marketing mails.

- Be wary of email sending behavior. Find a way to trickle the rate at which the bulk mail is being sent to Hosted Email Security. If possible, send them in batches and only send several mails per minute.

- Use a smart host for sending the bulk email messages. Especially when the bulk email message is going to just one or a few domains, configuring the mail server to deliver the mails directly to the destination mail server could be a better option. Most MTAs and mail servers have a way to do this.
- Use a 3rd party bulk email service provider for sending out these types of mails. This will eliminate the need to relay them through Hosted Email Security.
- Use DNS query for routing bulk mails. If possible, configure the mail server or application sending the bulk email messages to use DNS MX query when delivering them.
- Separate mails by purpose (user mails vs. bulk mails) and use different email address, domain, and/or IP address for each function. This way, bulk mail routing can be configured separately without affecting the user email messages.

Different mail servers and MTAs have different ways of implementing smarthost and mail routing. Consult your application's documentation for details.

It is important to note that when sending the bulk email messages directly to recipients, it is also possible that your own IP may be listed to the blocked list of different IP Reputation and RBL service providers. Always consider regulating your own email sending rate to avoid being blacklisted.

Rate Limiting is not unique to Hosted Email Security. Every public email service provider implements some form of rate limiting for the same exact reasons stated above. Protecting the service and keeping it available at all times is the responsibility of both the service provider and its users/customers.

5.10 License Renewal

When renewing license for Hosted Email Security, make sure that the new Activation Code is properly added to the existing Customer Licensing Portal (CLP) account. DO NOT create a new account because this will not be associated to your domain registered in Hosted Email Security. In the long run, it may lead to improper license mapping and possible service deactivation.

A Hosted Email Security account is tied to only one Registration and Activation key.

If you have an existing Hosted Email Security account that has been renewed, do the following to ensure that the renewal is successful.

1. Go to the Customer Licensing Portal (CLP).
2. Log in using your Hosted Email Security username and password.
3. Under **My Products/Services**, check **Expiration Date** and make sure it reflects the correct license end date.

Once you have renewed your Hosted Email Security, the records are updated accordingly. There is no web interface for renewing the activation code from the Hosted Email Security administrator console. The changes are done on the CLP database, so you will not have to do any action other than purchasing the renewal.

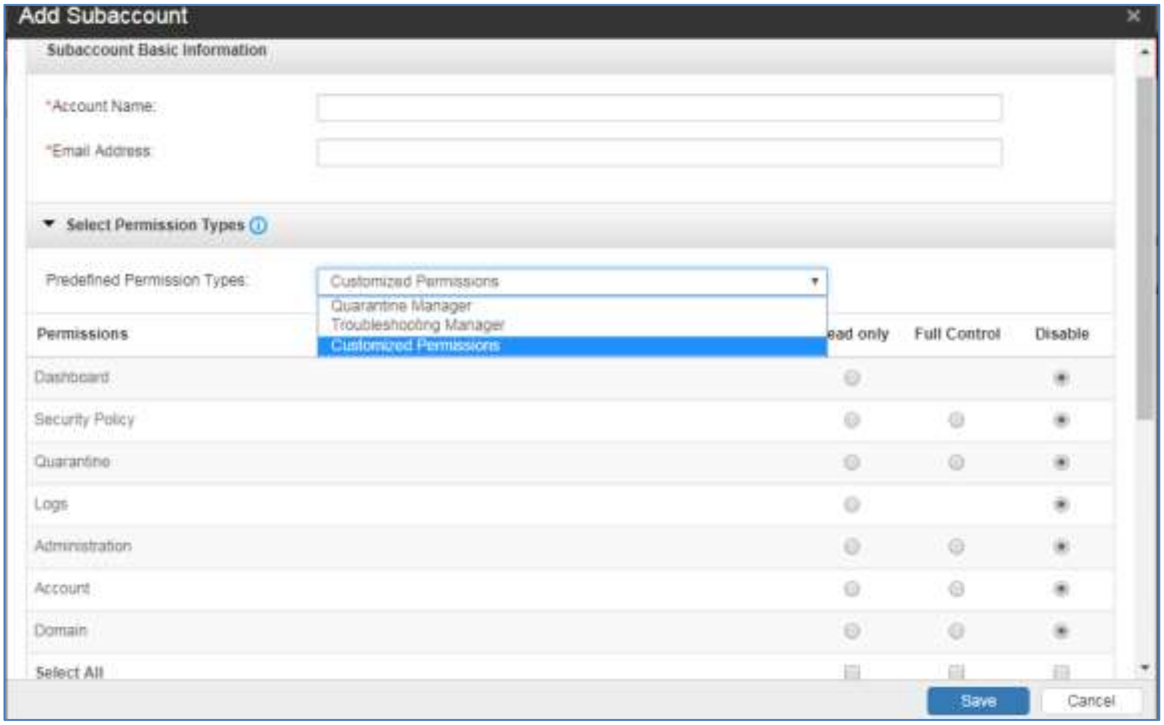
5.11 Account Management

Hosted Email Security customers will have one main account that they can use to login to Customer Licensing Portal and update their license information. This same account can also be used to login to Hosted Email Security administrator console to provision domains and make configuration changes.

This main account also has the capability to create sub-accounts that can be assigned to other Hosted Email Security administrators. The sub-account can be given permission to one or more of the main account's registered domains. In addition, Role Based Access Control settings are available to provide granular permissions to the sub-account, granting or denying access to certain parts of the administrator console.

To create a sub-account:

1. Go to **Administration** > **Account Management**.
2. Click **Add**. The **Add Subaccount** screen appears.
3. Configure the following information on the screen:
   - Subaccount Basic Information: add the user **Account Name** and **Email Address**.
   - Select Permission Types: select permissions from the **Predefined Permission Types** list, or configure permissions for each of the feature manually.



Add Subaccount

Subaccount Basic Information

*Account Name:

*Email Address:

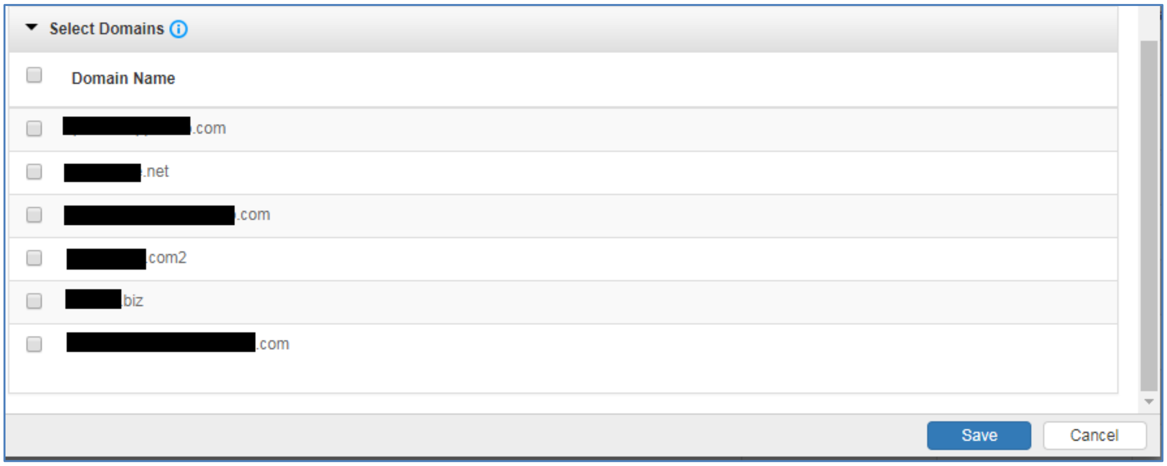
▾ Select Permission Types

Predefined Permission Types: Customized Permissions ▾

- Quarantine Manager
- Troubleshooting Manager
- Customized Permissions

Permissions	ead only	Full Control	Disable
Dashboard	○		●
Security Policy	○	○	●
Quarantine	○	○	●
Logs	○		●
Administration	○	○	●
Account	○	○	●
Domain	○	○	●
Select All	□	□	□

4. Select Domains: select domains that the account can use and update.



Select Domains

□	Domain Name
□	[redacted].com
□	[redacted].net
□	[redacted].com
□	[redacted]com2
□	[redacted]biz
□	[redacted].com

5. Click **Save**.
6. Hosted Email Security generates a password and sends it to the newly created account owner through an email message.

It is highly recommended that administrators are provided their own sub-accounts rather than sharing a single account between multiple administrators. Sub-accounts do not only provide a convenient way of providing least amount of privilege required by the administrator, it also allows proper auditing when necessary.

Administrator logins and configuration changes can be tracked from **Logs > Audit Log** page of the administrator console.

5.12 End-User Management

End-User Management provides a way for customers using Active Directory to enable single sign-on for End-User Quarantine (EUQ) Console access. By enabling and configuring this feature, end users will not need to manage and memorize an additional account name and password for EUQ. Instead, they will use their own Active Directory credentials to login to EUQ console.

This provides both convenience and additional security for the end user accounts.

Refer to the About Single Sign-On section of the Administrator's Guide for the complete details on how to configure this feature.