Trend Micro™ Hosted Email Security

Best Practice Guide

Authors: Henry Martin
Editor: Nancy Jiang
Release Date: March 2018
Edited for sensitive terms by Sherwin Lara Paran on December 22, 2020

Chapter 1: Introduction 1
Chapter 2: Provisioning 2
2.1: On-Premise Mail Server 3
2.2: Microsoft Office 365 4
2.3: Google G Suite 4
2.4: Provisioning Additional Domains 4
Chapter 3: Inbound Mail Protection 6
3.1: Malware and 0-Day Threats Protection 7
3.2: Spam Protection 8
3.2.1: Configure IP Reputation Setting 8
3.2.2: Add filters to default spam and phish policy 9
3.2.3: Enable Time-Of-Click Protection 11
3.2.4: Enable the Newletter or Spam-like Policy 11
3.3: Spoofed Email Protection 12
3.3.1: Configure the list of High Profile Users for Business Email Compromise filter 13
3.3.2: Create an Anti-Spoof Policy 13
3.3.3: Enable SPF Checking 16
3.3.4: Enable DKIM Signature Checking 21
3.3.5: Enable DMARC 22
3.3.6: Approved and Blocked Senders 22
3.3.7: Sender Filter Settings 23
3.4: Backscatter Spam and Directory Harvest Attacks (DHA) Email Messages 23
3.5: Incoming Transport Layer Security (TLS) 24
3.6: Ransomware Protection 25
Chapter 4: Outbound Mail Protection 26
4.1: Using Outbound Filtering 26
4.2: Policies 26
4.2.1: Outbound Virus Policy 27
4.2.2: Add additional outbound spam and phish policy 27
4.3: Outgoing Transport Layer Security 28
4.4: Publish SPF record in DNS 28
4.5: DomainKeys Identified Mail Signing 28
4.6: Email Encryption 30
Chapter 5: Other Features and Settings 32
5.1: Dashboard 32
5.2: Approved and Blocked Senders 32
5.3: Sender Filter Settings 32
5.4: Regular Expressions 33
5.5: Scan Exceptions 33
5.6: Message Retention and Quarantine Management 34
5.7: Quarantine Digest 36
5.8: General Order of Evaluation 37
5.9: Bulk Email Sending 37
5.10: License Renewal 39
5.11: Account Management 39

5.12: End-User Management 40

Chapter 1: Introduction

Trend Micro Hosted Email Security (HES) 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: Provisioning

Hosted Email Security can be provisioned to work with any type of email environment. Regardless if the organization is using a traditional on-premise 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.

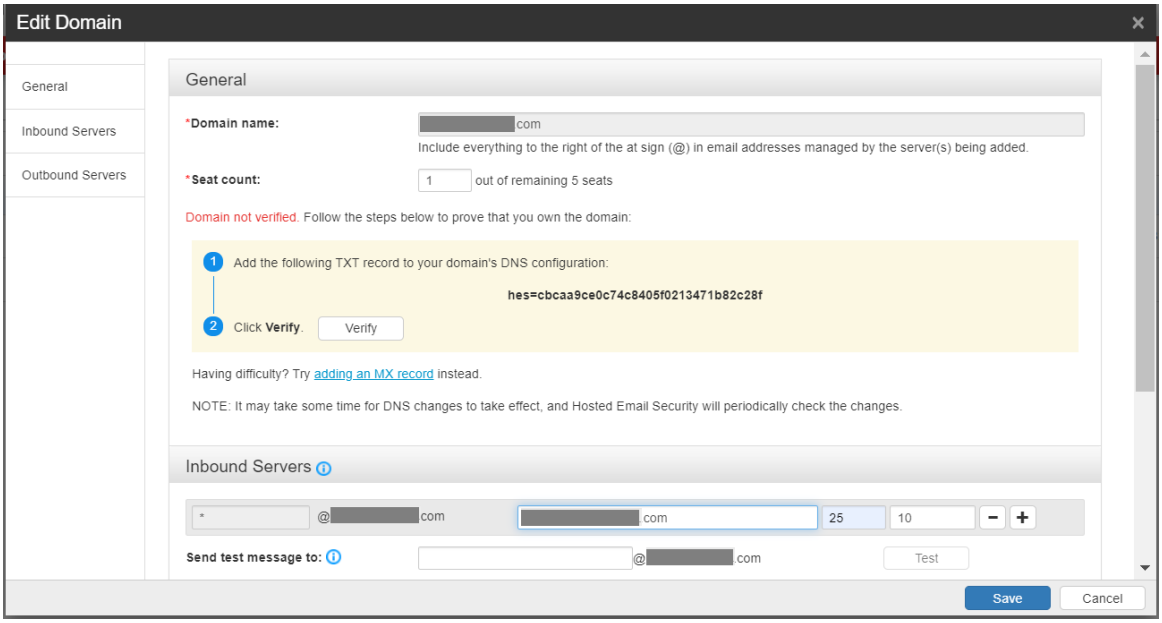


TABLE 2.1: Example of Initial Domain Configuration Window

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 policies.

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-Premise 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.

Ensure that the configured MX record is correct:

Europe, the Middle East and Africa:
in.hes.trendmicro.eu

All Other Regions:
in.hes.trendmicro.com

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

Europe, the Middle East and Africa:
• 52.48.127.192/26
• 52.58.62.192/26
• 52.58.63.0/25

All Other Regions:
• 54.86.63.64/26
• 54.219.188.0/26
• 54.219.191.0/25

In addition, if the organization's firewall, mail transfer agent (MTA) or mail server is configured to check any IP Reputation 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 checking on the firewall, mail transfer agent or mail server. Hosted Email Security has its own IP Reputation list using Trend Micro Email Reputation Services.

Disable SPF checking on the email gateway, mail transfer agent or mail server only when this feature is 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 being used, setup the mail server to send all outgoing email messages to Hosted Email Security by configuring a smarthost. Point the smarthost/relay connector to:

• Europe, the Middle East and Africa:
relay.hes.trendmicro.eu

- All Other Regions:
  relay.hes.trendmicro.com

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

2.2. Microsoft Office 365

For customers using Office 365, it is required to configure the inbound and outbound connectors to work with Hosted Email Security.

For the detailed steps, read and follow Knowledge Base article 1101972.

TIP: Do not forget to follow the steps under Inbound Servers and Outbound Servers which can be found on the Edit Domain window.

If the outbound protection is enabled, it is highly recommended to setup the DNS SPF TXT Record to ensure that the Hosted Email Security managed domain will not be used for malicious activities:

If there is no existing DNS SPF TXT record, the information below should be used:

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

For existing DNS SPF TXT record, only add include: spf.hes.trendmicro.com.

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.

In order to integrate HES and G Suite, follow the steps on Knowledge Base article 1098849.

TIP: It is highly advised to setup the DNS SPF TXT record when outbound protected is enabled.

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

Chapter 3: Inbound Mail Protection

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

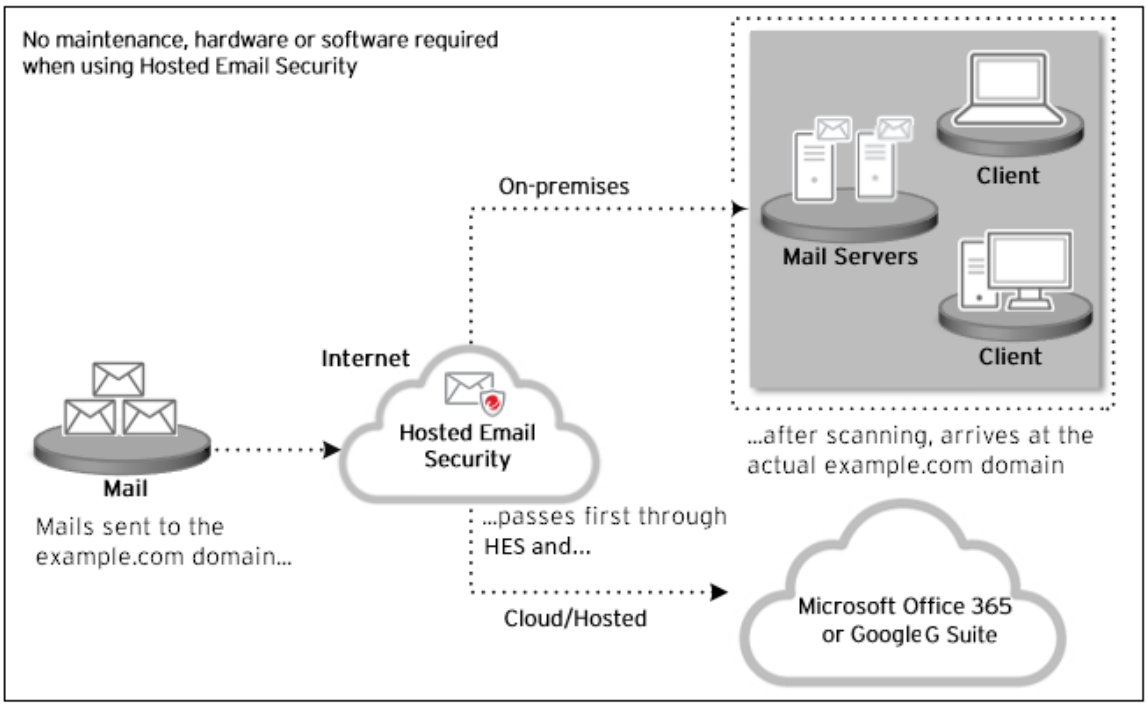


FIGURE 3.1: Inbound Mail Flow Diagram

Step	Description
1	The originating mail transfer agent (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.

TABLE 3.1: Inbound Mail Flow Process

Step	Description
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.

TABLE 3.1: Inbound Mail Flow Process

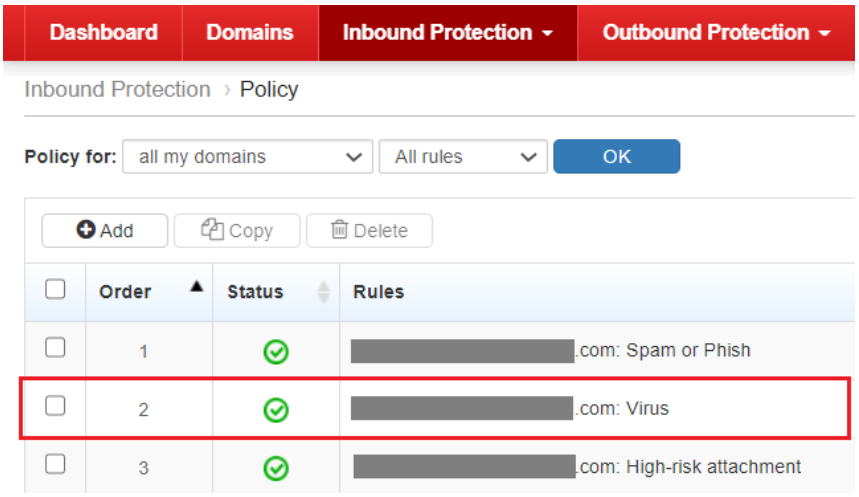
Inbound Mail Protection best practice includes enabling and configuring protection against different types of threats such as malware, spam, spoofed email messages, and even ransomware.

3.1. Malware and O-Day Threats Protection

By default, the virus policy is already set to "Quarantine" action. If it was modified to a different action other than "Delete", set it back to "Delete" or "Quarantine" action to avoid any malware to enter your environment.

1. Log on to the Hosted Email Security administrator console.

2. Go to **Inbound Protection > Policy and look for the Virus policy**.



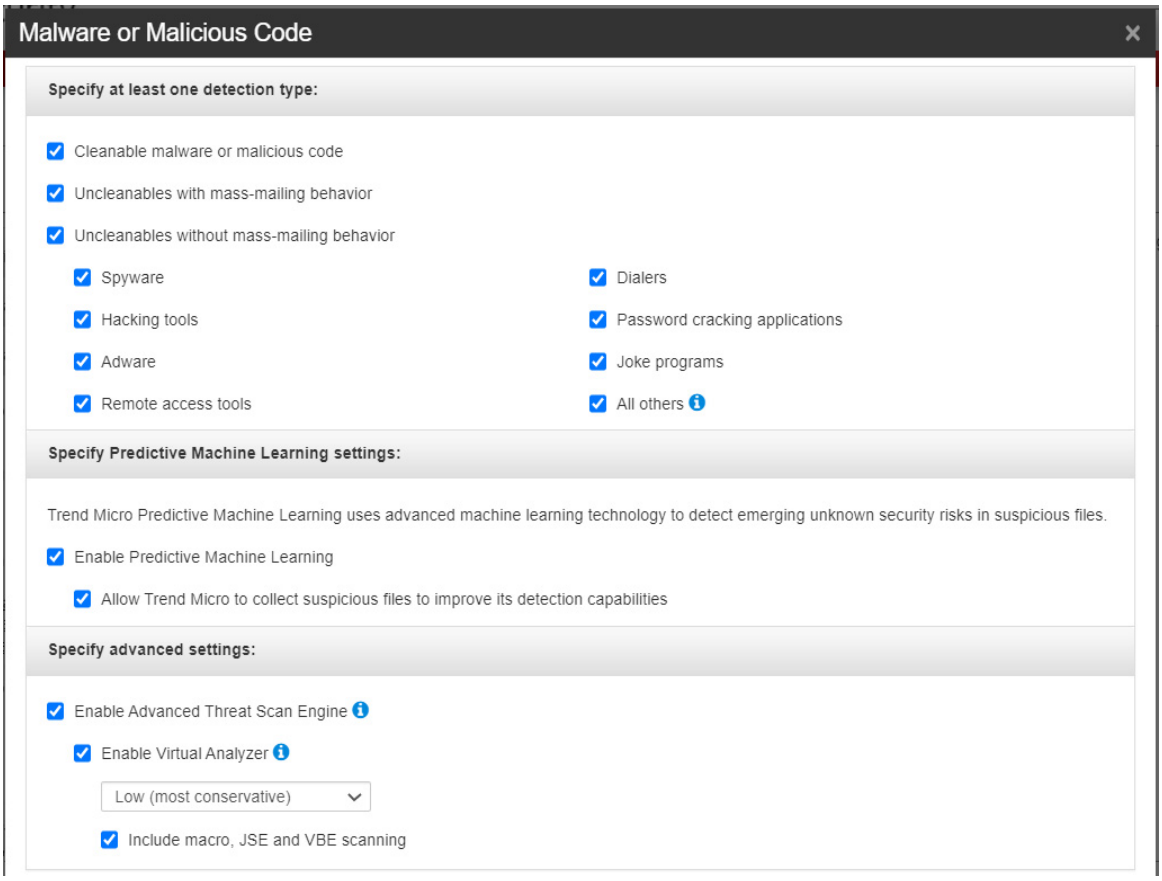
3. Make sure the action is set to **"Quarantine"** or **"Delete"**.

4. Ensure that the policy applies to **"ALL users"** and there are no "Senders and Recipients Exceptions".

5. Under Scanning Criteria, click **malware or malicious code**. Afterwards, ensure **all malware detection types** are checked.

6. Enable **Virtual Analyzer and include macro, JSE and VBE scanning**. This provides protection against zero-day and unknown threats by running suspicious files on a sandbox environment.

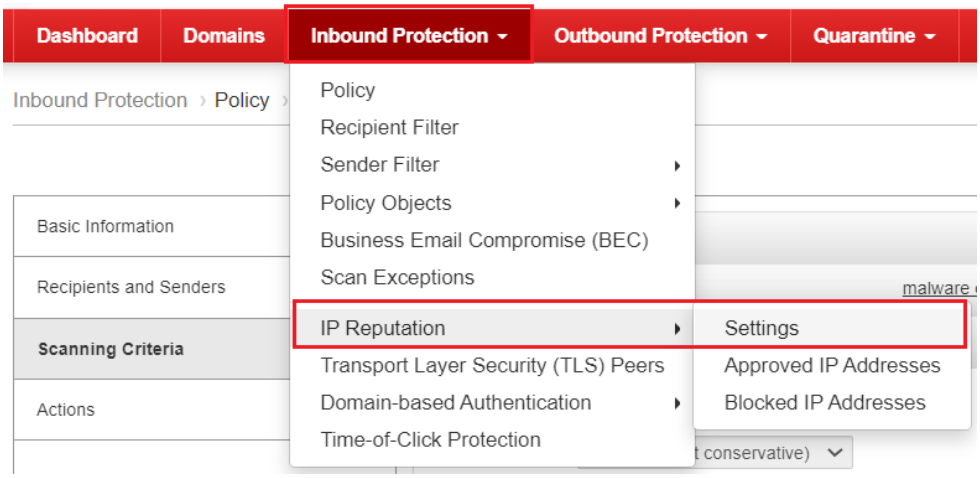
7. Enable **Predictive Machine Learning and allow Trend Micro to collect suspicious files** to improve its detection capabilities.



3.2. Spam Protection

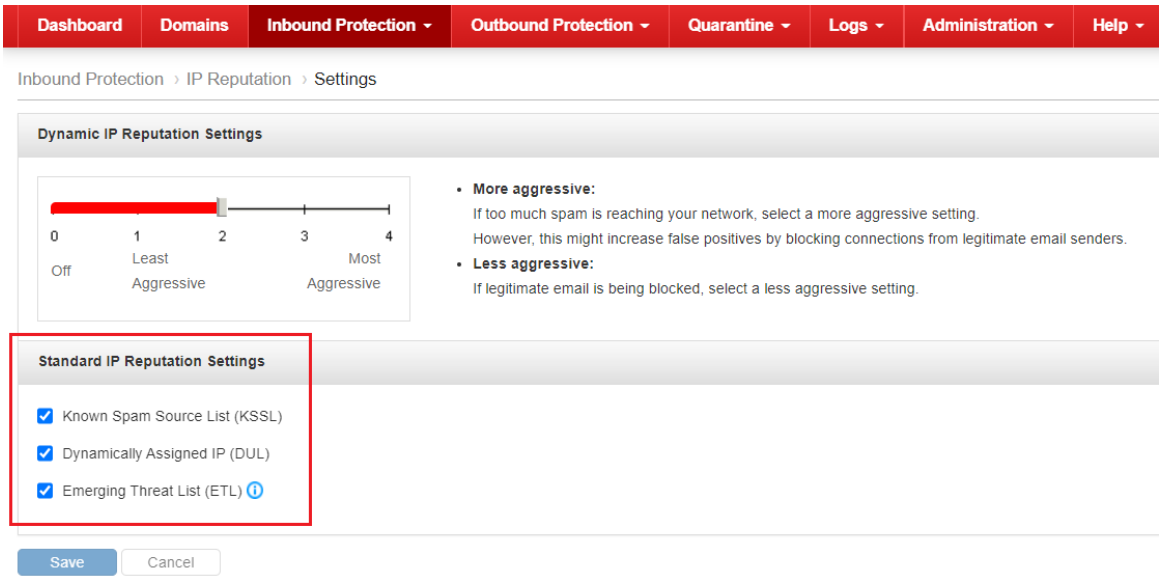
3.2.1. Configure IP Reputation Setting

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



2. Set the aggressiveness level based on the need of your organization. If you are constantly under attack, increasing the aggressiveness level is highly recommended.

3. Enable all 3 IP Reputation checking (KSSL, DUL and ETL).

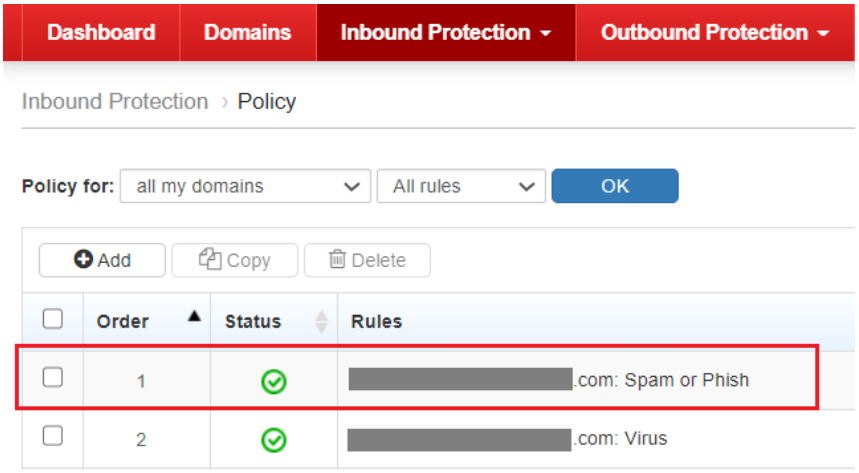


3.2.2. Add filters to default spam and phish policy

Depending on the amount of spam messages that your organization is receiving, it may be necessary to increase the spam detection level and enable social engineering attack.

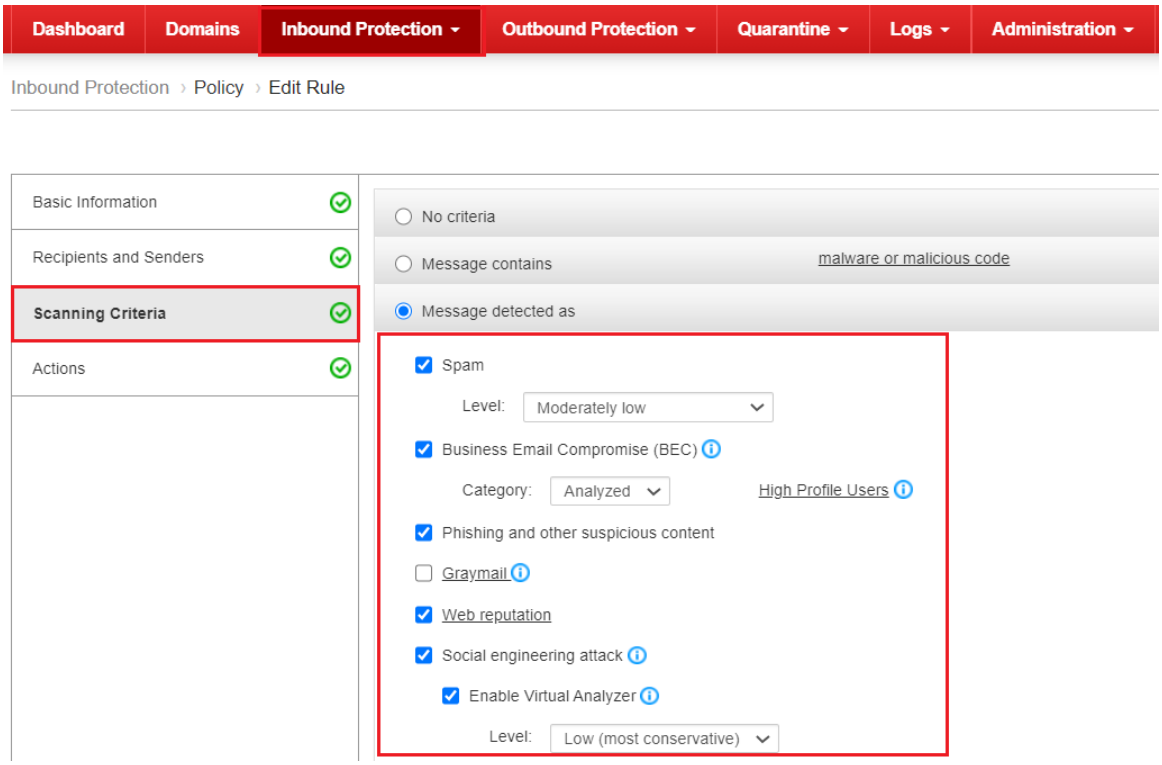
1. Log on to the Hosted Email Security administrator console.

2. Go to **Inbound Protection > Policy and look for the Spam or Phish policy for each managed domain**.



3. Click **Scanning Criteria**.

4. Check **all boxes, except Graymail,** then set Spam check to a higher level. Graymails are covered by a different policy which is "Newsletter or spam-like".



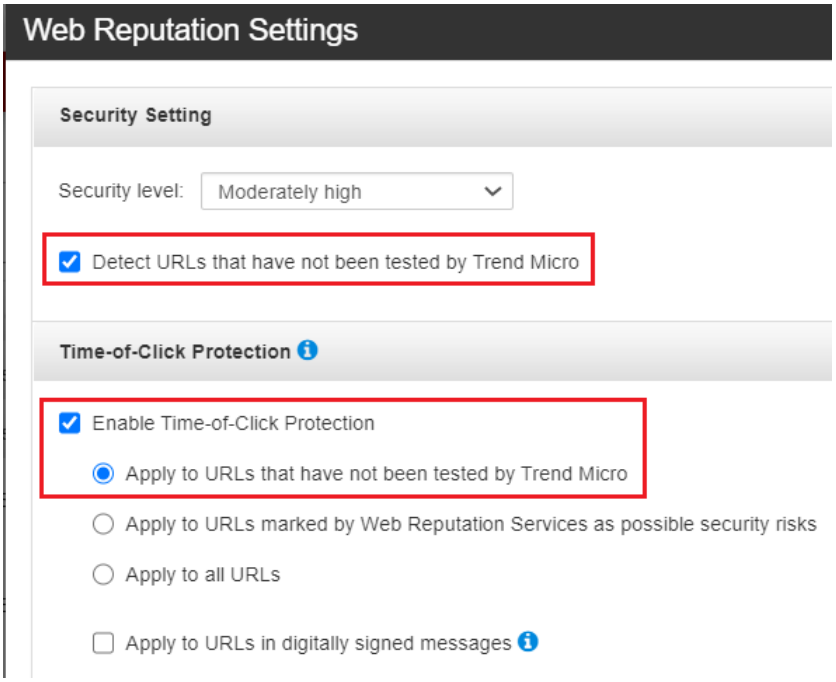
NOTE: Setting Spam check to a higher level may lead to more false positives. However, it may also reduce false negative messages and avoid malicious messages. If Virtual Analyzer is enabled, Hosted Email Security performs observation and analysis on samples in a closed environment. Advanced analysis 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 URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click and will block them if they are malicious to protect the users.

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

2. Select the following 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



3. Click **Save** then **Submit**.

See Configuring Time-of-Click Protection Settings.

3.2.4. Enable the Newletter or Spam-like Policy

Hosted Email Security includes a default policy named "Newsletter or spam-like". This policy scans specifically for Graymail, which is referred as the unsolicited bulk email messages that are not spam.

This policy should be enabled and a scan action should be configured based on organizations' need or preference.

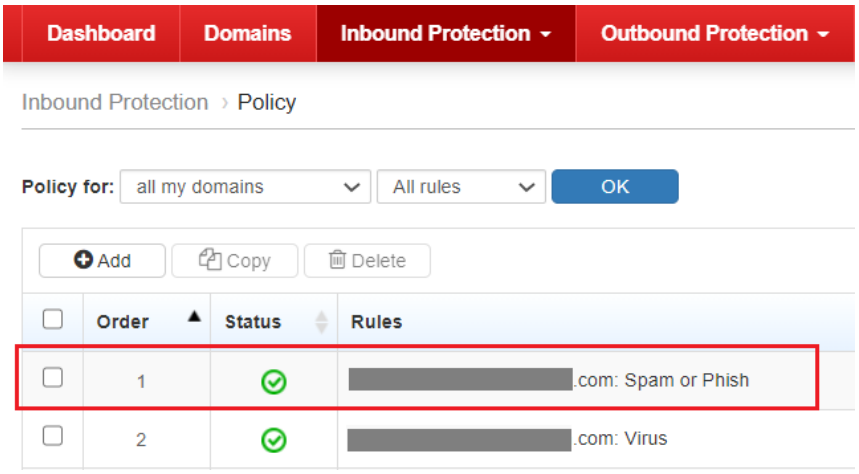
Some organizations prefer to allow newsletters to pass through while some do not.

3.3. Spoofed Email Protection

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

1. Log on to the Hosted Email Security administrator console.

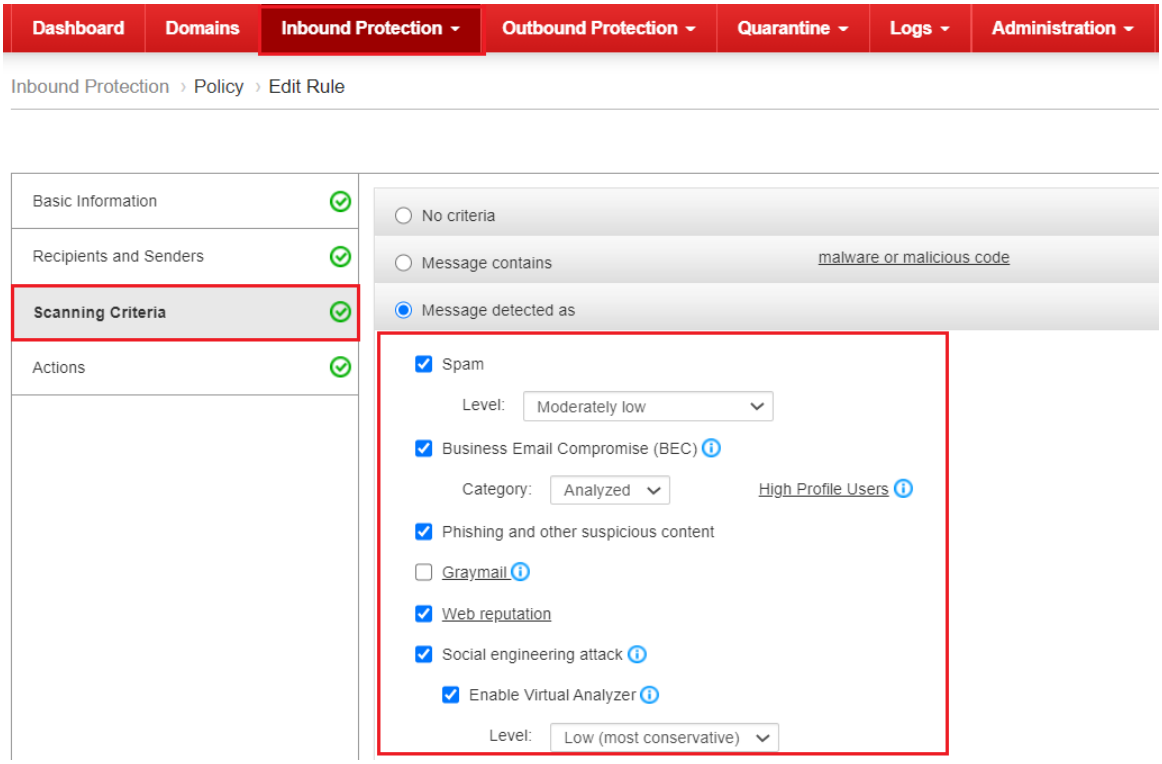
2. Go to **Inbound Protection > Policy and look for the Spam or Phish policy for each managed domain**.



3. Click **Scanning Criteria**.

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.

3.3.1. Configure the list of High Profile Users for Business Email Compromise filter

Business Email Compromise (BEC) is a type of spoofed email attack which 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. It 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.

3.3.2. Create an Anti-Spoof Policy

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

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.

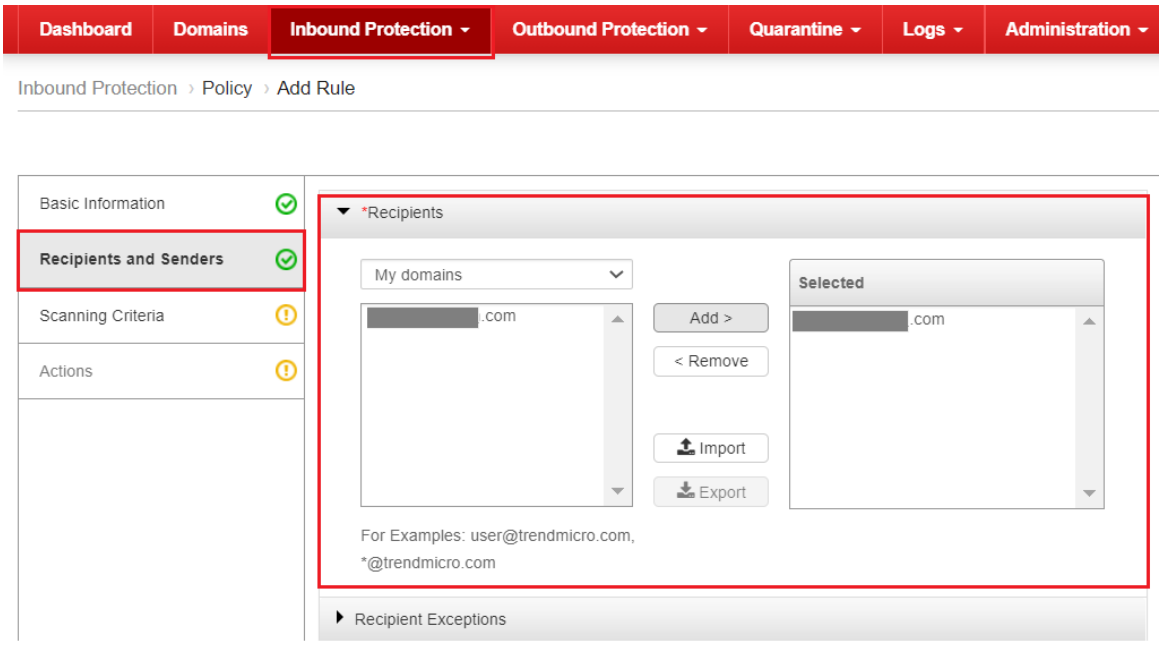
WARNING: Warning: Make sure intra-domain email messages are not routed to the Internet.

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

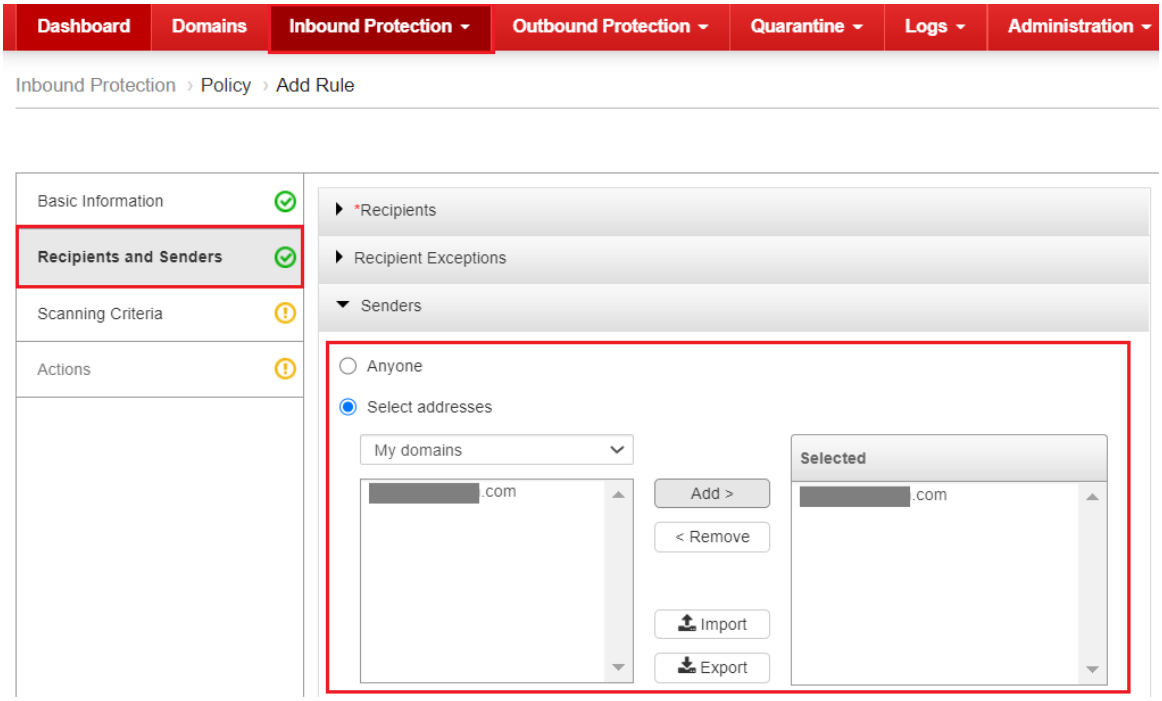
2. Go to **Inbound Protection > Policy and click Add**.

3. Type name of the rule you are creating (e.g. Anti-Spoof Policy).

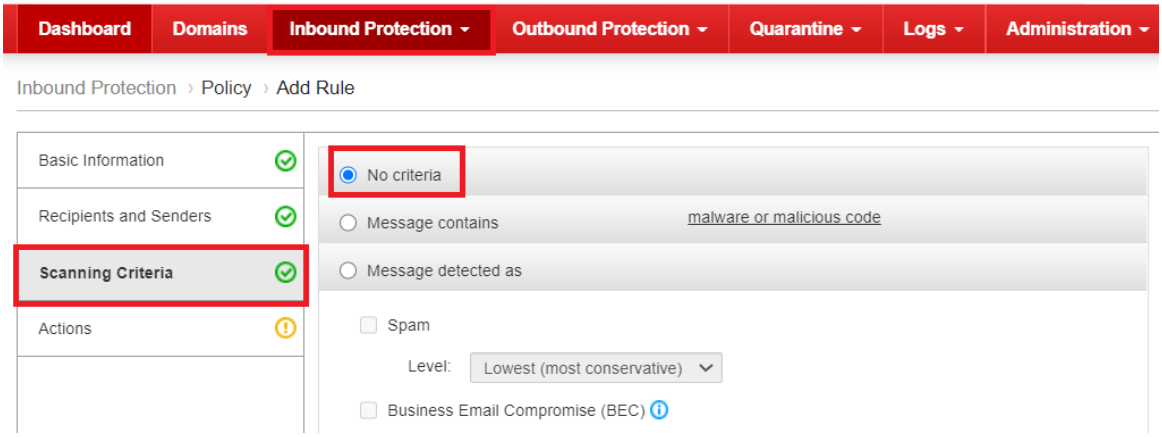
4. Go to **Recipients and Senders > Recipients**, add your domain.



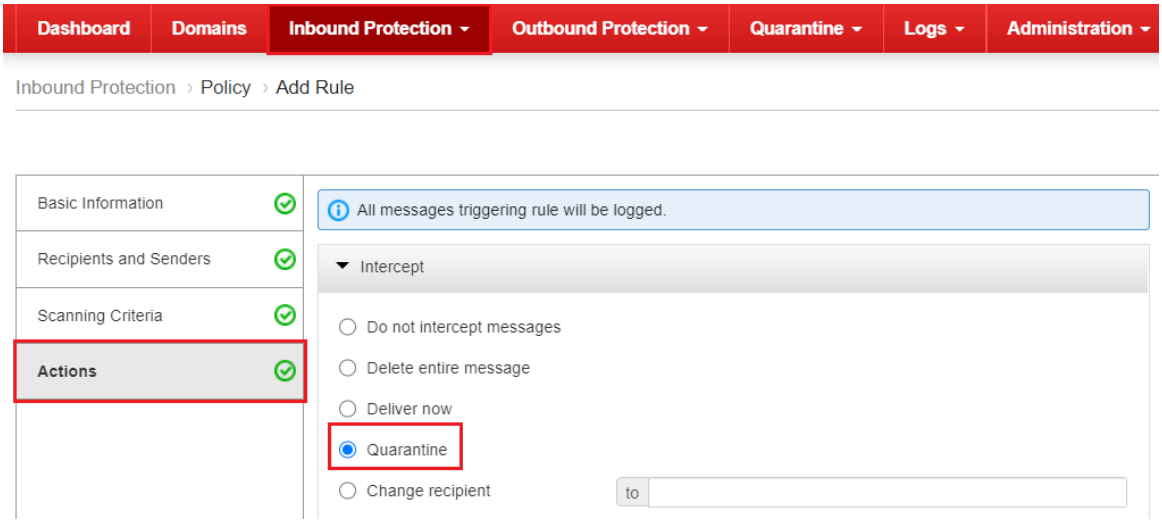
5. Go to **Recipients and Senders > Senders**, add the same domain.



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



7. Under Actions, select **"Quarantine"** in order to have access to review the filtered email messages.



8. Click the **Submit** button.

3.3.3. Enable SPF Checking

Sender Policy Framework (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.

Sender Policy Framework requires the owner of a domain to specify and publish their email sending policy in SPF record of their 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.

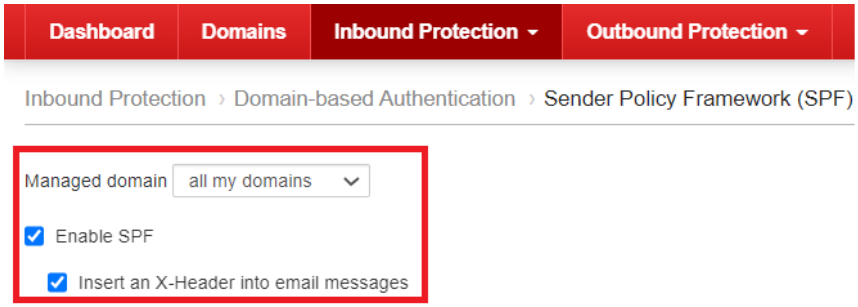
1. Enable SPF Checking in Hosted Email Security then create the SPF TXT record for your domain if you are using Hosted Email Security outbound relay.

    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 **"Insert X-Header into email messages"**.



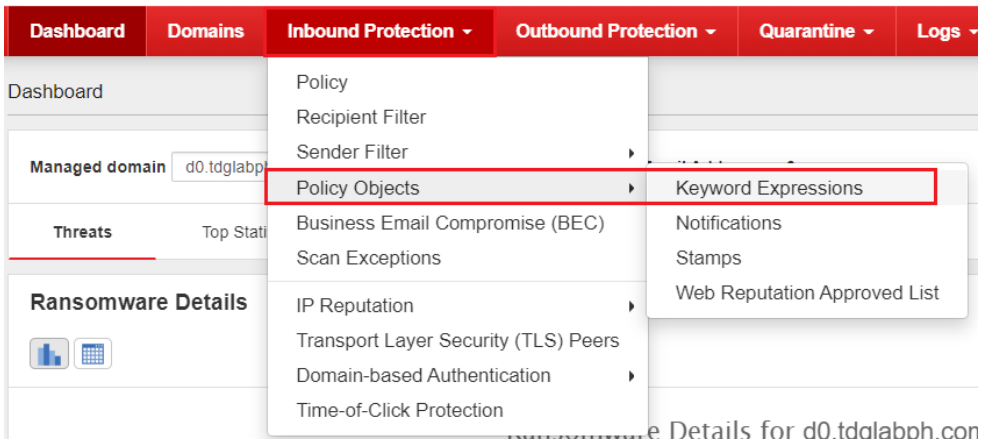
2. Create a policy to track email messages tagged by Hosted Email Security SPF check due to SoftFail.

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

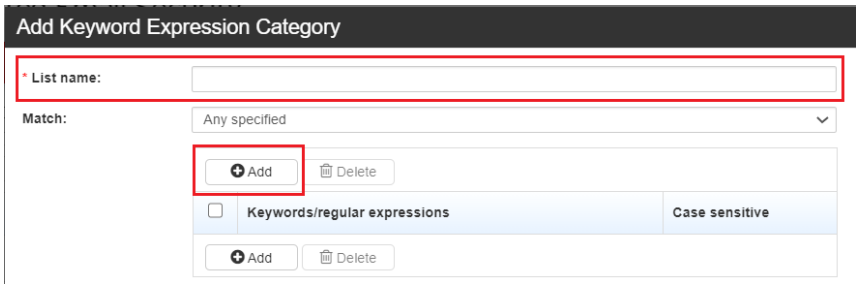
NOTE: Emails that fail the SPF checking due to hard fail will already be blocked and logged by Hosted Email Security. Therefore, there is a need to create an additional policy to track them.

a. Log on to the administrator console.

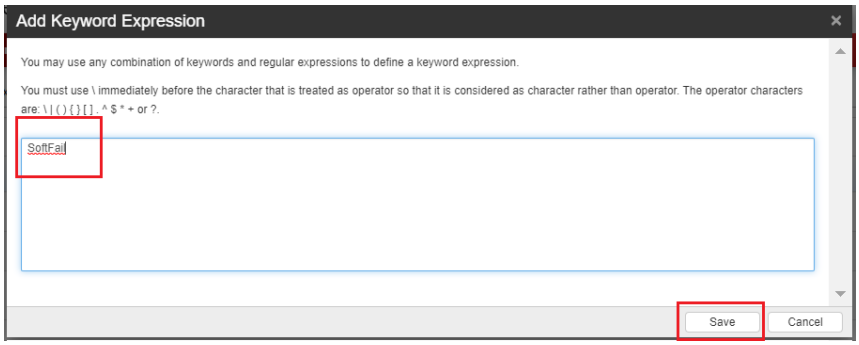
b. Go to **Inbound Protection > Policy Objects > Keyword Expressions**.



c. Click Add and then, type a name for the keyword list (e.g. SPF Soft Fail). To confirm, click the **Add** button.



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



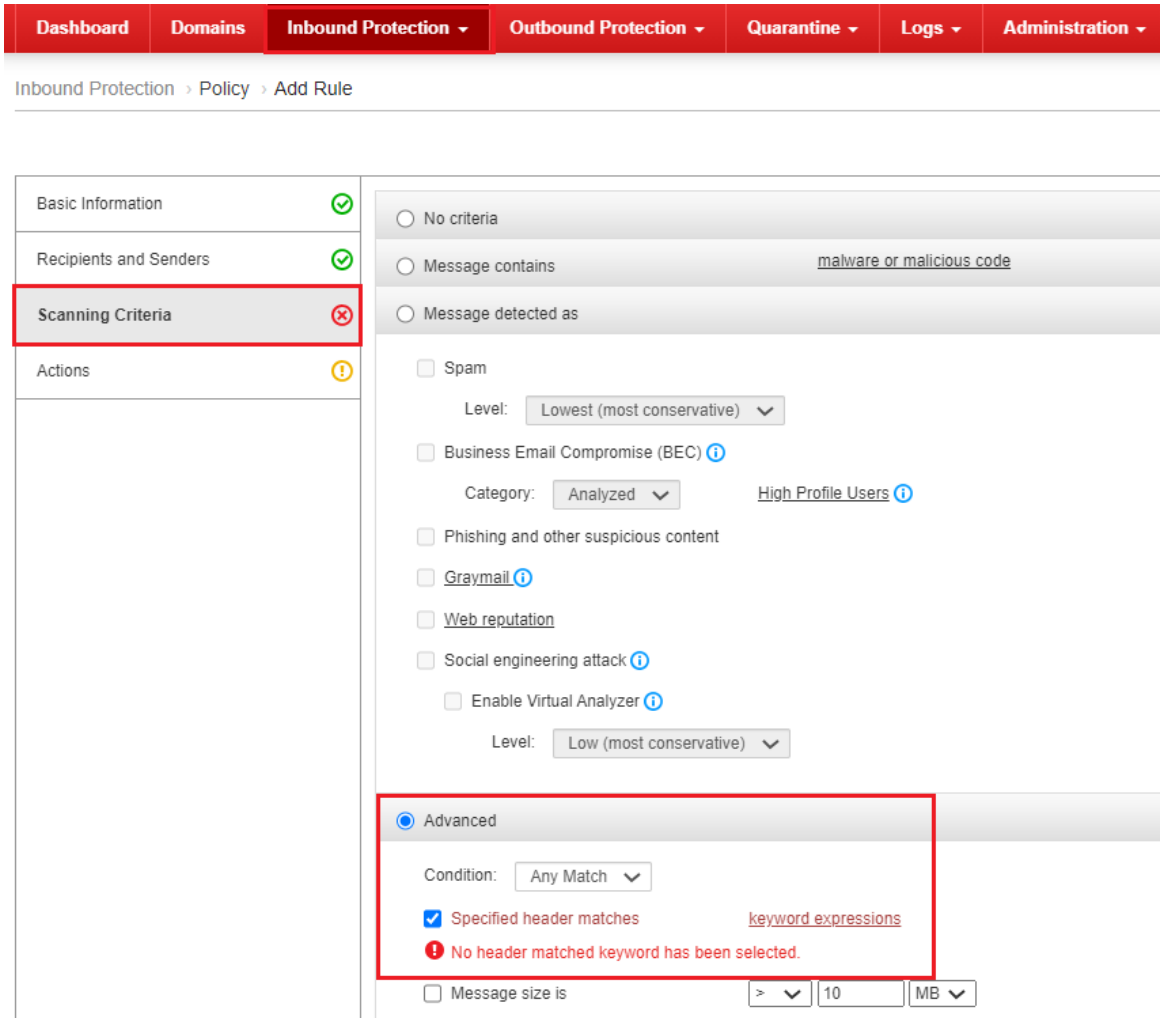
e. Go to **Inbound Protection > Policy and click Add**.

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

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

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

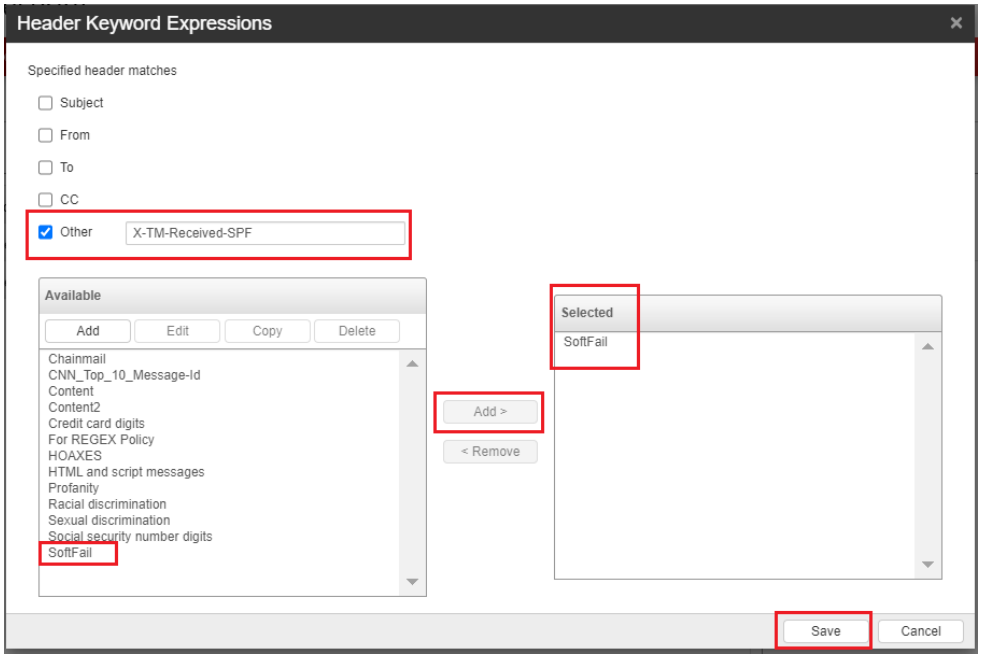
i. Click **keyword expressions** beside Specified header matches.



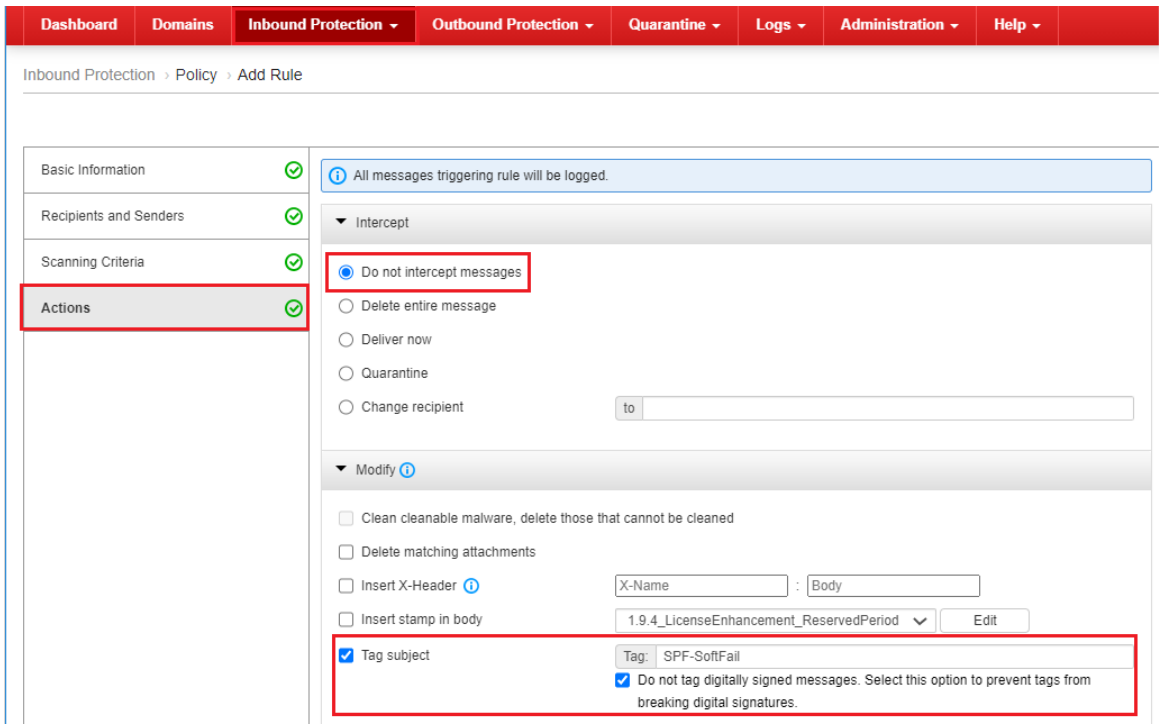
j. Check **Other** and type the keyword **"X-TM-Received-SPF"**.

k. From the list of Available keyword lists, find the list that you previously created. Select it then click on the **Add** button to move it to the Selected list.

l. Click the **Save** button.



m. Under Actions, select your preferred action. If your goal is only to log or track emails with SoftFail SPF result, select **"Do not intercept messages"**. Another option is to enable the Tag subject action and type the tag that you want to use.



n. Click the **Submit** button.

3.3.4. 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 within 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.

Moreover, the administrator can identify **"Enforced Peers"**, which is a list of domains that must have DKIM signatures on their emails. 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 DomainKeys Identified Mail Signature Verification:

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

2. Click **Add**. The Add DKIM Verification Settings window will pop up.

3. Select a specific recipient domain from the Domain Name drop-down list.

4. Select **Enable DKIM verification**.

5. Select **Insert an X-Header into email messages** if preferred.

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-TMAuthentication Results:dkim=fail; No verified signatures

6. Under Intercept, select an action that you want to follow when a message fails DKIM verification.
   - Do not intercept messages
   - Delete entire message
   - Quarantine

7. Under Tag and Notify, select further actions that you want to take on the message.
   - Tag subject
     Tags can be customized. When selecting the Tag subject action, note the following:
     – This action may destroy the existing DKIM signatures in email messages which may lead to DKIM verification failure by the downstream mail server.

– To prevent tags from breaking digital signatures, select **Do not tag digitally signed messages**.

- Send notification

8. Under Enforced Peers, add enforced peers to enforce DKIM verification for specific sender domains.
   a. Click **Add**.
   b. Specify a sender domain name then click **Add**. All email messages from the specified domain must pass verification according to the DKIM standard. Otherwise, messages will be taken action.

9. Click **Add** to finish adding the DKIM verification settings.

3.3.5. 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 & 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.

3.3.6. 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.

Approved Senders

1. 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 checking and IP Reputation checking.

2. Do not put an internal email addresses or domain in the Approved Senders list.

Blocked Senders

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

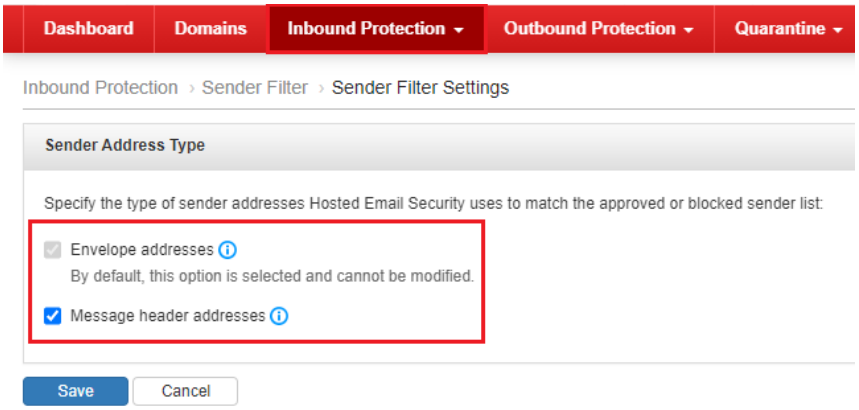
2. If no internal email message passes through Hosted Email Security, internal domains may be added in the Blocked Senders list to protect against envelope sender spoofing.

3. Limit the amount of entries to a manageable number.

3.3.7. 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.



For more details, refer to this Knowledge Base article 1117423.

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

See About Directory Management.

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

1. Go to **Inbound Protection > Recipient Filter**.

2. Look for your domain on the list.

3. 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.

TIP: 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 mail transfer agents (MTAs) 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 the Hosted Email Security administrator console, go to **Inbound Protection > Transport Layer Security (TLS) Peers**.

2. Select your domain from the Managed Domain drop-down list then click the **Add** button.

3. Type the address of your own or partner MTA that must use TLS in all its communication.

4. Under Security level, select **Mandatory**.

5. Click the **Save** button.

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, follow the topics below:

1. Enable IP reputation setting. For the procedure, refer to this Knowledge Base article 1101535.

2. Ensure that the Spam and Phish inbound policy is enabled. This includes Web Reputation Services (WRS), new born URL handling and Trend Micro Locality Sensitive Hash (TLSH). Follow the instructions on Knowledge Base article 1052815.

3. Block file types commonly used by Ransomware. To do this, refer to Knowledge Base article 1099636.

4. 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 **Enable Virtual Analyzer** to identify threats. Then select Include macro scanning during advanced analysis.

5. Click the **Save** button.

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.

Chapter 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.

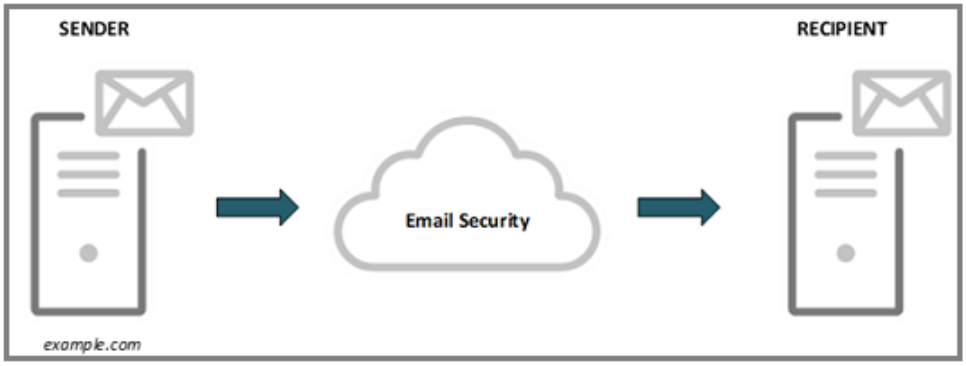


FIGURE 4.1: Outbound Mail Flow Diagram

Step	Description
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.

TABLE 4.1: Outbound Mail Flow Process

4.2. Policies

Hosted Email Security has separate policies applied to outbound email messages. Depending on organizational 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

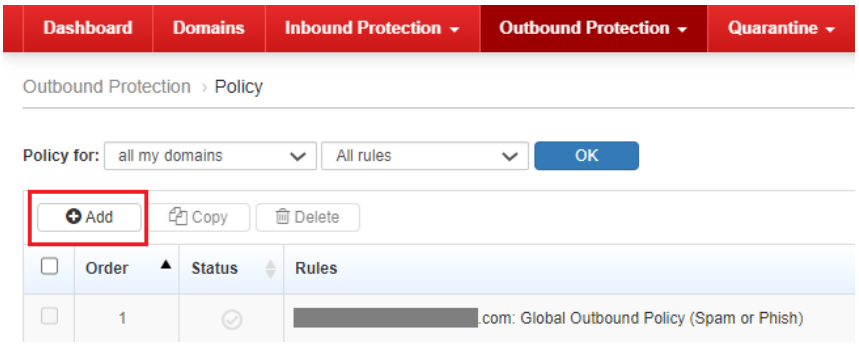
Hosted Email Security Global Outbound Policy (Spam or Phish) is a default rule to avoid outbound spam and prevent Hosted Email Security outbound servers from being blocked by 3rd party Known Spam Source List (KSSL). The policy cannot be edited and they are activated by default for all domains.

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. Login to Hosted Email Security administrator console.

2. Go to **Outbound Protection > Policy** then click **Add**.



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

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

5. Under Scanning Criteria, select **all boxes** (Spam, Phishing and other suspicious content, Web Reputation). You can adjust the spam detection level based on your needs.

NOTE: Setting spam check higher might lead to more false positive but it can also reduce false negative email messages and avoid malicious email messages.

6. Under Actions, select your preferred action such as **"Quarantine"** and click **Submit**.

4.3. Outgoing Transport Layer Security

Similar to Incoming Transport Layer Security (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 mail transfer agent.

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.

1. From Hosted Email Security administrator console, go to **Outbound Protection > Transport Layer Security (TLS) Peers**.

2. Click **Add**.

3. Type the domain name in the TLS Peer text box.

4. Under Security level, select **Mandatory**.

5. Click **Save**.

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.

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. DomainKeys Identified Mail Signing

By enabling DomainKeys Identified Mail (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. Below are the steps:

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

2. Click **Add** then the Add DKIM Signing Settings screen appears.

3. Select a specific sender domain from the Domain name drop-down list.

4. Select **Enable DKIM signing**.

5. 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 it 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/
WCkQ5WRWJ4Ln64EssFPQojX0yNIOTgjrchcK0/IKX1eRvZzbX8kErmgT5hvEys9tDoW7iG/
zAZUqhmtgDuha8ULFknxsvrMhPsVs3jSjX373bBWtOgI+izFCH+MU6KznyJZGcckEsPkS3ffy
KrOZQAMpv6zu28tx2P8mPMnCqzjxMmPXiBZTJ19/
MkWAU1VHD39bUVByu0dImQdEodBqcPxyev/pBh++kNpvIpuBnnaXtZCKAYBtqt8HF6w/
eimyStcPYtHpmBY43stCTg5Kr3ON1KRuCN3o/
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-201705241492 3._domainkey	**IN**	**TXT**	**"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEF AAOCAQ8AMIIBCgKCAQEA5m HBjC/ WCkQ5WRWJ4Ln64EssFPQojX0y NIOTgjrchcKO/ IKX1eRvZzbX8kErmgT5hvEys9tD oW7iG/ zAZUqhmtgDuha8ULFknxsvrMhPs Vs3jSjX373bBWtOgI+izFCH+MU6 KznyJZGcckEsPkS3ffy"**
TM-DKIM-2017052414923._domainkey	IN	TXT	"KrOZQAMpv6zu28tx2P8mPMnCq zjxMmPXiBZTJ19/ MkWAU1VHD39bUVByu0dImQd EodBqcPxyev/ pBh+ +kNpvIpuBnnaXtZCKAYBtqt8HF6 w/ eimyStcPYtHpmBY43stCTg5Kr3O N1KRuCN3o/ vLUKGPgCPLyjLVh5beme1BRouy xU42s8OLuBEcU9umpKhQIDAQ AB"

TABLE 4.2: Divided DNS DKIM TXT Record Information

6. 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 re-wrapping.

   - **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.

7. 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 need to configure rules to apply encryption as a rule action.

Special rules can be created in order for Hosted Email Security to only encrypt email messages between selected people. To use email encryption:

1. From the Hosted Email Security administrator console, go to **Outbound Protection > Policy**.

2. Click **Add**.

3. Type a name for the policy.

4. Under Recipients and Senders, specify the sender and recipient addresses of email messages that should be encrypted. Exceptions can be specified but not required.

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.

5. 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**.

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

7. 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.

Chapter 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 checking. Ensure to put trusted addresses only.

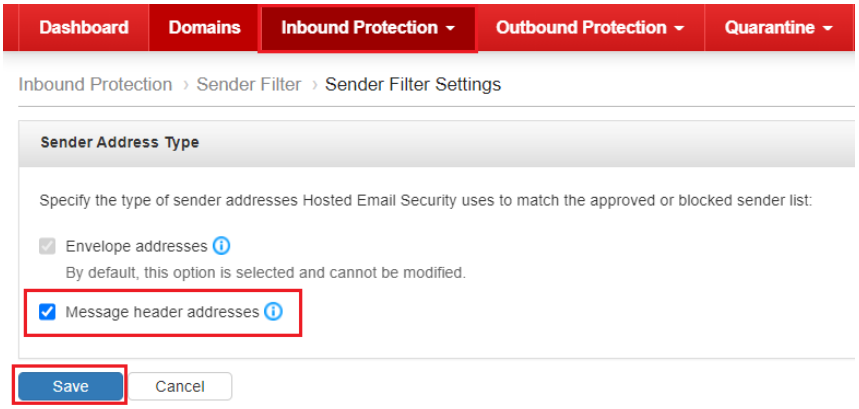
c. Never put an internal email address or domain in the Approved Senders list to avoid spoofed email attacks.

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.

1. From the Hosted Email Security administration console, go to **Inbound Protection > Sender Filter > Sender Filter Settings**.

2. Enable the checkbox for Message header addresses.



3. Click the **Save** button.

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 Knowledge Base article 1117423.

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.

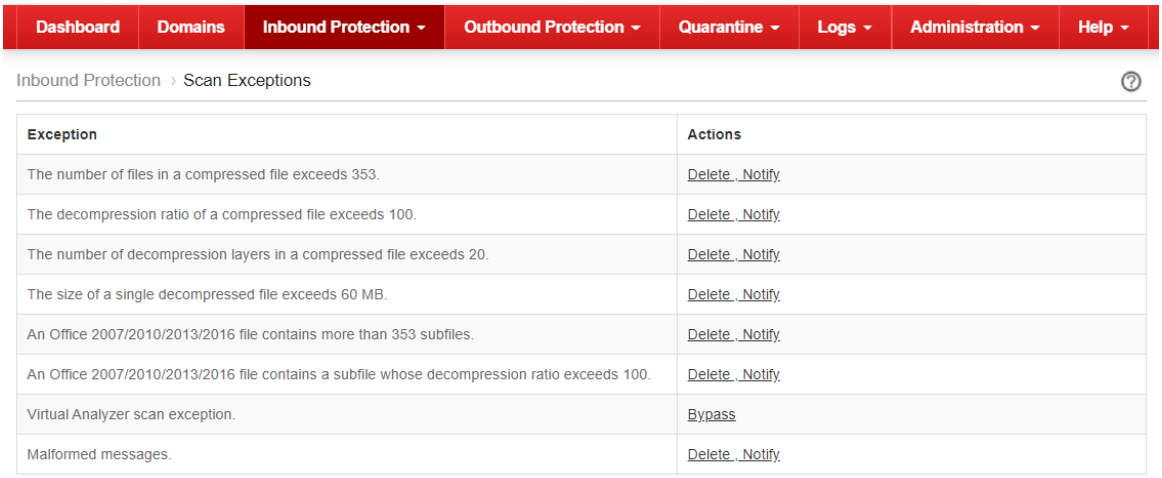
Using long and complex regular expression are more prone to errors and false detection. Therefore, it is recommended to split long and complex keyword expression to several entries.

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**.



Sometimes, normal files may trigger the scan exceptions due to the number of files inside a compressed or Microsoft 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 then choose to deliver it.

5.6. Message Retention and Quarantine Management

The following table shows message retention information:

Item	Retention Period
Quarantined email messages	30 days
Message tracking logs	90 days
Message queue when customer MTA is unavailable	Up to 10 days

TABLE 5.1: Retention Period Summary

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. Login to the Hosted Email Security administrator console.

2. In the Dates fields, select a range of dates. 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, either Incoming or Outgoing.

4. Type your search criteria into one or more of the following fields:
- Recipient
- Sender
- Subject

NOTE: 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, you may 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: The Download button is only available on the Quarantine Query Details page.

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:

Europe, the Middle East and Africa:
https://euq.hes.trendmicro.eu

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.

Process	Description
1	Sender email addresses filtering - the 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 - the 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 - the 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.

TABLE 5.2: General Order of Evaluation Process

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 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.

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 Known Spam Source Listing**: 3rd party IP Reputation or Known Spam Source List (KSSL) 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 KSSL 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 smarthost 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 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 Known Spam Source List (KSSL) service providers. Always consider regulating your own email sending rate to avoid being blocked.

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**. 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. Therefore, you will not have to do any action other than purchasing the renewal.

5.11. Account Management

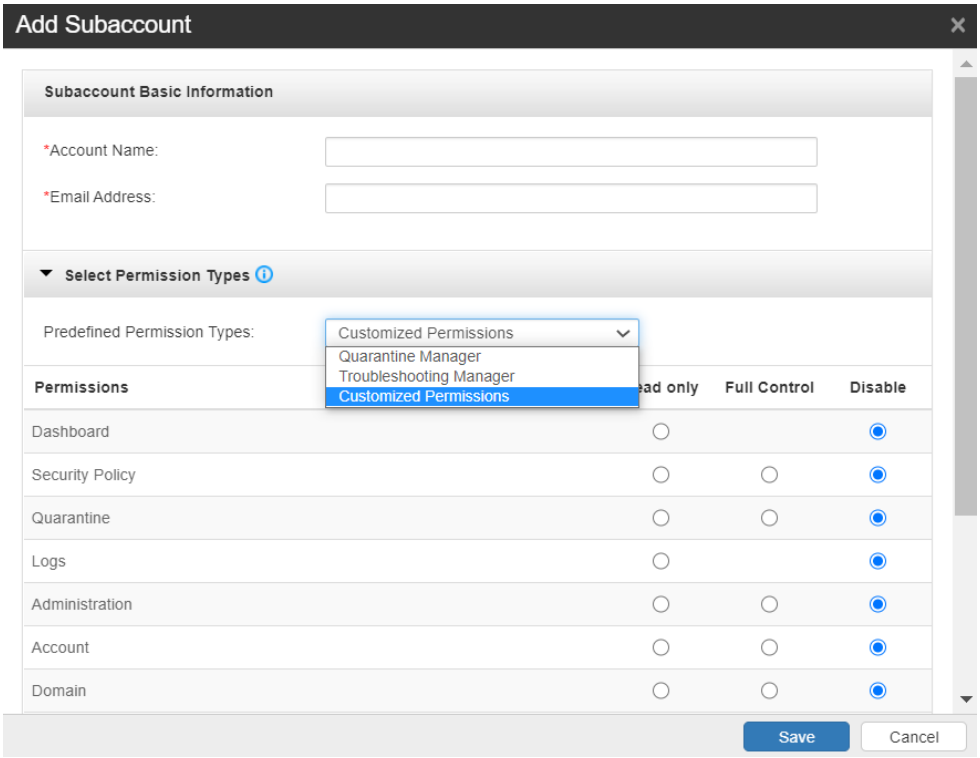
Hosted Email Security customers will have one main account that they can use to login to Customer Licensing Portal and update their license information. This same account can also be used to login to Hosted Email Security administrator console to provision domains and make configuration changes.

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.
   - **Select Domains**: Select domains that the account can use and update.

4. Click **Save**.

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