Trend Micro™ Email Security

Best Practice Guide

Authors: Fritz Gerald Reyes and Jason Zhang
Contributor: Jia-Bing Cheng
Editor: Sherwin Lara Paran
Official Release Date: March 13, 2020

Chapter 1: Product Overview

Trend Micro Email Security (TMEMS) 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.

Trend Micro Email Security deployment is easy, requiring organizations to simply redirect their MX records. The default settings are strategically optimized to provide immediate protection upon deployment.

Changes in configuration can be done to fit the organization's requirement which allows flexibility.

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

1.1. Mail Flow Diagrams for On-Premise Mail Server

Inbound:

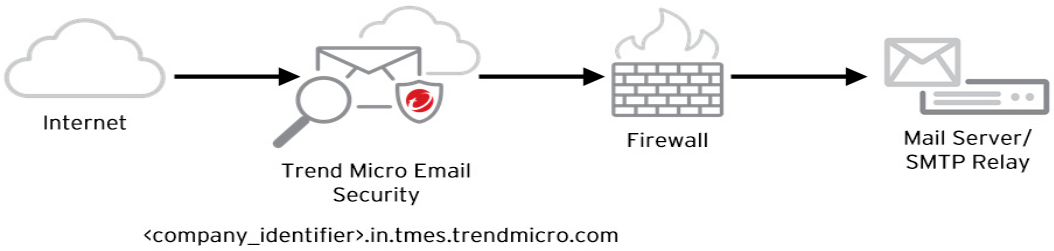


FIGURE 1.1.1: Inbound Mail Flow Diagram

Outbound:

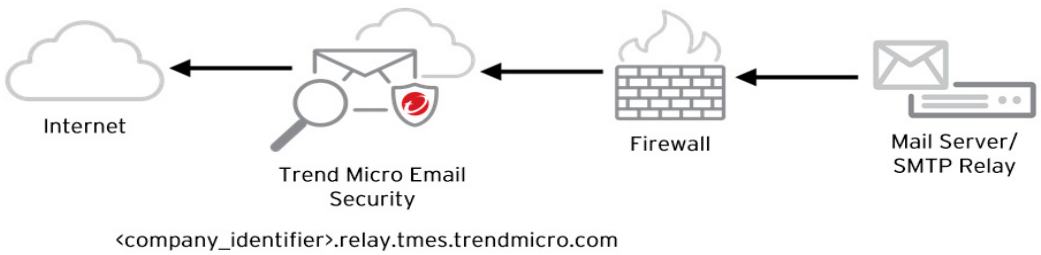


FIGURE 1.1.2: Outbound Mail Flow Diagram

NOTE: Sample Fully Qualified Domains Name (FQDN) above is used for TMEMS US/JP site. New sites added will have different FQDN.

1.2. Comparison of HES and TMEMS

This table summarizes the feature differences between HES and TMEMS:

Feature	Hosted Email Security	Trend Micro Email Security Standard	Trend Micro Email Security Advanced
General Availability	Yes	Yes	Yes
All current Hosted Email Security features: anti-spam, anti-malware, etc.	Yes	Yes	Yes
Predictive Machine Learning to detect malware	Yes	Yes	Yes
Email Encryption and Data Loss Prevention	Yes	Yes	Yes
Macrowave: Enhanced detection of malicious macros in documents	No	Yes	Yes
Anti-Phishing: Scans URL within file attachments	No	Yes	Yes
Mail Tracking performance enhancements – Amazon Web Services ElasticSearch	No	Yes	Yes
Mail Tracking Logs search window	7 Days	30 Days	60 Days
Mail Tracking Logs search conditions	Limited	Full	Full
Mail Tracking Logs search results exportable	No	Yes	Yes
Policy Events Logs search window	7 Days	30 Days	60 Days
Policy Events Logs search results exportable	No	Yes	Yes
URL Click Tracking Logs search results exportable	No	Yes	Yes
Mail Queue enhancements – Amazon Simple Queue Services	No	Yes	Yes
Directory Integration: Azure Active Directory, Microsoft Active Directory, OpenLDAP, IBM Domino	No	Yes	Yes

TABLE 1.1: Feature Differences

Feature	Hosted Email Security	Trend Micro Email Security Standard	Trend Micro Email Security Advanced
Connected Threat Defense: Consumes file and URL Indicators of Compromise from Trend Micro Control Manager	No	Yes	Yes
End User Quarantine auto-merge accounts based on directory	No	Yes	Yes
SAML / Okta for Single Sign-on and Multi-Factor Authentication	No	Yes	Yes
Reports in PDF of blocked email threats	No	Yes	Yes
Syslog for exporting logs	No	Yes	Yes
Email Spool for Disaster Recovery	Yes	Yes	Yes
Email Continuity for Disaster Recovery	No	No	Yes
Business Email Compromise detection by Writing Style with Trend Micro Cloud App Security Artificial Intelligence mode	No	No	Yes
File Sandbox	Yes	No	Yes
URL Sandbox	No	No	Yes
Email maximum size (MB)	50	50	50
Combine user mailbox and aliases into single quarantine view	Manual	Auto	Auto
Scan password protected files by password extraction	No	No	Yes
Trend Micro Remote Manager for Resellers	Yes	Yes	Yes
In Smart Protection Complete, Worry Free Business Security Advanced, Worry Free Services Advanced	Yes	Yes	No
In Smart Protection for Office 365	Not Applicable	No	Yes

TABLE 1.1: Feature Differences

TIP: For more details, refer to Available License Versions.

Chapter 2: Provisioning and Deprovisioning

Trend Micro 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 that are hosted in Office 365 or Google G Suite, it is a great choice for keeping malicious email messages and attachments out of your network.

Before adding a domain, customer needs to input their first name, last name, contact information, and other necessary information.

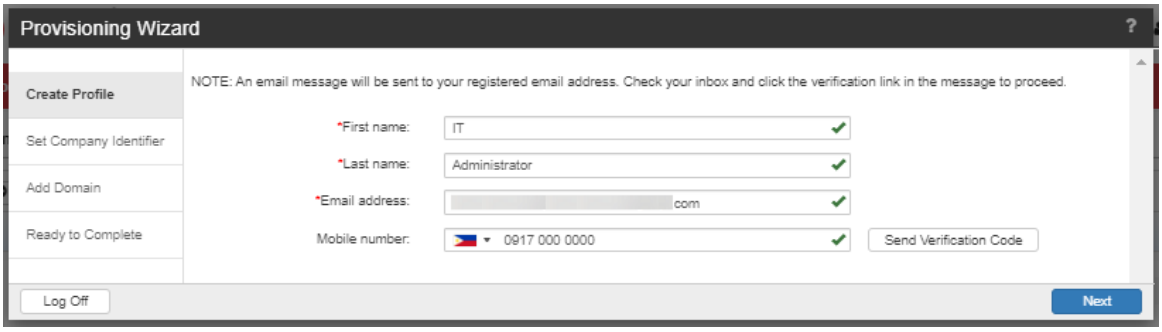


FIGURE 2.1: Example of Create Profile Window

Provisioning starts with adding your domain name in the Trend Micro Email Security administrator console then identifying the inbound servers to where the scanned email messages will be relayed.

Outbound filtering can be enabled optionally. 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 action. 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.

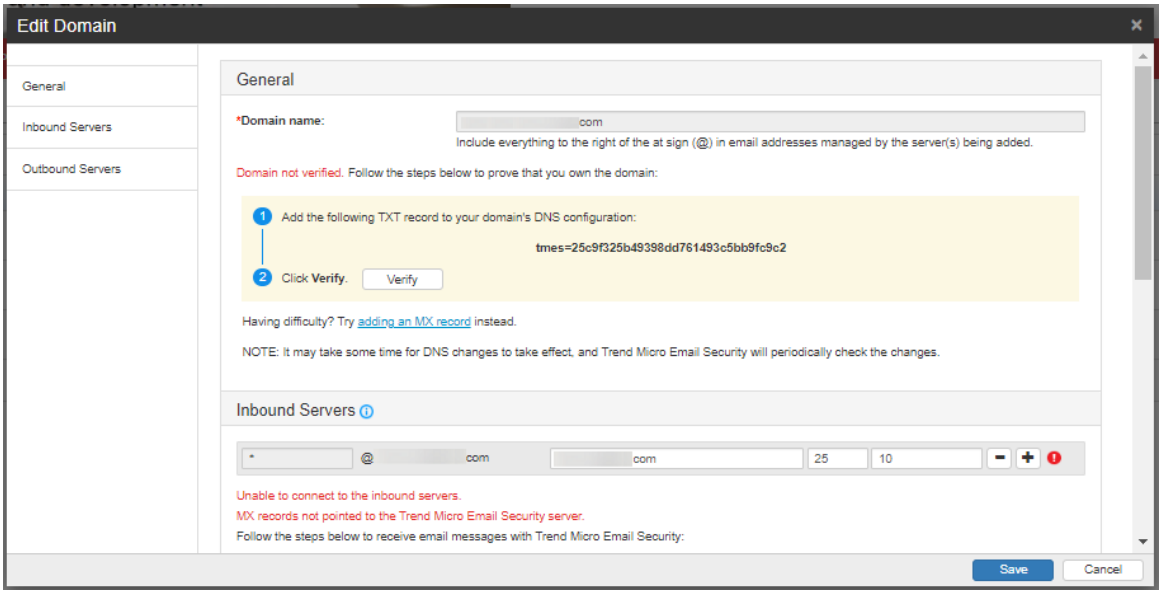


FIGURE 2.2: Example of Initial Domain Configuration Window

Refer to the "Configuring a Domain" section in the Administrator's Guide for details about this procedure.

It is important to note that email messages for the domain cannot be routed through Trend Micro Email Security while the domain status is at "Configuration Required". Once the domain status is shown as "Completed", then you can start using Trend Micro 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 ensure that no attacker can bypass Trend Micro Email Security scanning.

Ensure that the configured MX record is correct:

- North America, Latin America and Asia Pacific:
<company_identifier>.in.tmes.trendmicro.com

- Europe, the Middle East and Africa:
<company_identifier>.in.tmes.trendmicro.eu

- Australia and New Zealand:
<company_identifier>.in.tmes-anz.trendmicro.com

- Japan:
<company_identifier>.in.tmems-jp.trendmicro.com

To achieve this, configure the firewall and/or mail server to accept email messages only from the following Trend Micro Email Security IP blocks:

North America, Latin America and Asia Pacific:
• 18.208.22.64/26
• 18.208.22.128/25
• 18.188.9.192/26
• 18.188.239.128/26

Europe, the Middle East and Africa:
• 18.185.115.0/25
• 18.185.115.128/26
• 34.253.238.128/26
• 34.253.238.192/26

Australia and New Zealand:
• 13.238.202.0/25
• 13.238.202.128/26

Japan:
• 18.176.203.128/26
• 18.176.203.192/26
• 18.177.156.0/26
• 18.177.156.64/26

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. Trend Micro 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 Trend Micro 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 Trend Micro Email Security outbound filtering is being used, setup the mail server to send all outgoing email messages to Trend Micro Email Security by configuring a smarthost. Point the smarthost/relay connector to:

• North America, Latin America and Asia Pacific:
<company_identifier>.relay.tmes.trendmicro.com

• Europe, the Middle East and Africa:
<company_identifier>.relay.tmes.trendmicro.eu

• Australia and New Zealand:
<company_identifier>.relay.tmes-anz.trendmicro.com

• Japan:
<company_identifier>.relay.tmems-jp.trendmicro.com

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

BEST PRACTICE: It is recommended to route outgoing emails to Trend Micro Email Security only. On the other hand, do not relay internal emails to Trend Micro Email Security.

2.2. Office 365

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

For the detailed steps, read and follow Knowledge Base article 000250836.

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 Trend Micro 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.tmes.trendmicro.com -all`

For existing DNS SPF TXT record, only add `include:spf.tmes.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 Trend Micro Email Security.

In order to integrate TMEMS and G Suite, follow the steps on Knowledge Base article 000250837.

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

2.4. Notification and Deprovisioning Process

Deprovision in this section refers to the process for soon-to-be-expired licenses. This is a mechanism to remind customers to purchase or renew license. Below diagram discusses about the different license lifecycle:

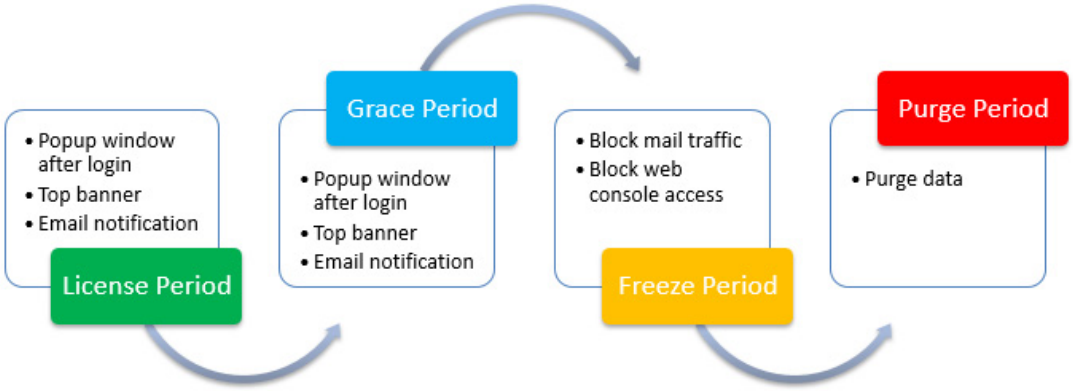


FIGURE 2.4.1: License Lifecycle

NOTE: The pop-up window can be seen by both license account and sub-account. Pop-up windows can be closed. Top banner cannot be closed.

2.4.1. License Period

The License Period is described by the table below:

Period Definition	Remind Condition	Remind Action
1. License is in valid period (Defined in Customer Licensing Portal (CLP) or Licensing Management Platform (LMP)) 2. Calculation: Current Time is before customer License Expiration Date	• Full License: starts 30 days before the license expiration date • Trial License: starts 5 days before the license expiration date • Auto-Renewal License: No reminder about the license period	• Pop-up window after administrator login • Top banner on each page in administrator console • Send notification to: – email address saved in account profile (either during provision or manually added) – email address synced from CLP or LMP

TABLE 2.1: License Period Summary

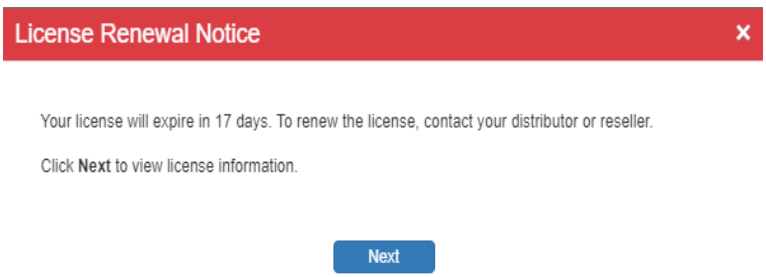


FIGURE 2.4.1.1: License Renewal Pop-up Notification

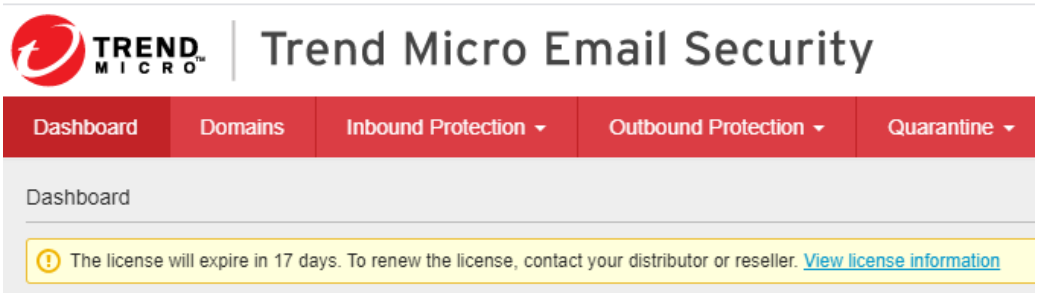


FIGURE 2.4.1.2: License Period Top Banner Notification

Your Trend Micro Email Security license will expire in 9 days. Please renew your license before it expires.

For more information, see "License Information" in the Online Help:
http://docs.trendmicro.com/en-us/enterprise/tmems/olh/license-management

Technical Support Website:
https://success.trendmicro.com/product-support/email-security

Best regards,
Trend Micro

FIGURE 2.4.1.3: License Period Email Notification

2.4.2. Grace Period

The Grace Period is described by the table below:

Period Definition	Remind Condition	Remind Action
1. License is in grace period (Defined in Customer Licensing Portal (CLP) or Licensing Management Platform (LMP)) 2. Calculation: Current Time is after License Expiration Date and before end of Grace Period 3. Grace Period is synchronized from CLP and LMP system **WARNING:** If grace period is more than 30 days, use the grace period sync from CLP (30days)/LMP (45days). Otherwise, the grace period is 30 days.	Starts during the grace period	• Pop-up window after administrator login • Top banner for each page in administrator console • Email notification to: – remind to purchase or renew license within the grace period – remind to change the MX record 2 days before the end of the grace period

TABLE 2.2: Grace Period Summary

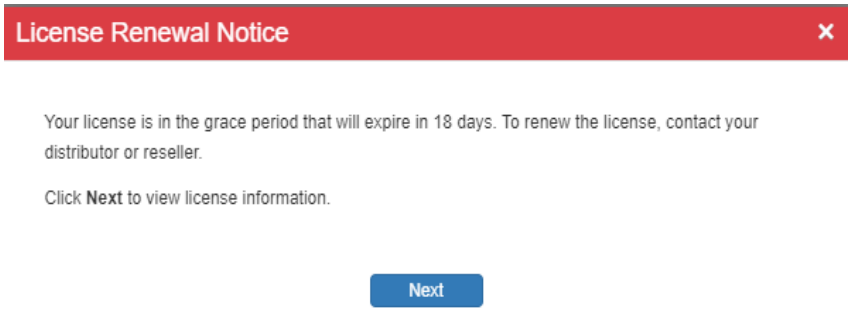


FIGURE 2.4.2.1: Grace Period Pop-up Notification

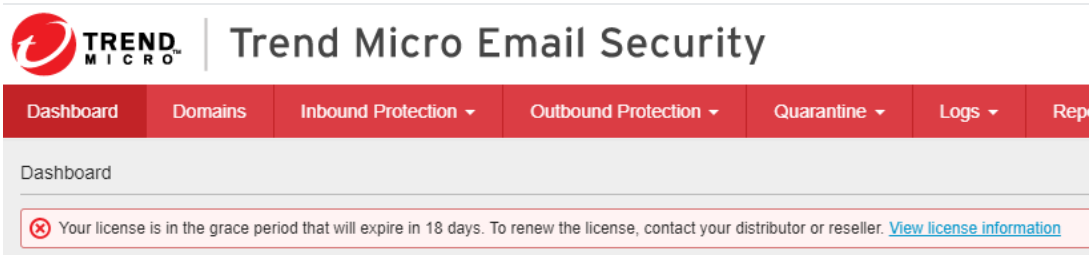


FIGURE 2.4.2.2: Grace Period Top Banner Notification

Your Trend Micro Email Security license is in the grace period that will expire in 26 days. Your service will be suspended after the grace period. Please renew your license before the grace period expires.

If you want to suspend this service, modify your MX record timely to avoid mail traffic interruption.

For more information, see "License Information" in the Online Help:
http://docs.trendmicro.com/en-us/enterprise/tmems/olh/license-management

Technical Support Website:
https://success.trendmicro.com/product-support/email-security

Best regards,
Trend Micro

FIGURE 2.4.2.3: Grace Period Email Notification Content

2.4.3. Freeze Period

The Freeze Period is described by the table below:

Period Definition	Remind Condition	Remind Action
30 days from the expiration of Grace Period	Starts after the grace period expiration then up to 30 days from the grace period expiration	• Block customer mail traffic • Disable domains in EMS backend • Block administrator and end user console access

TABLE 2.3: Freeze Period Summary

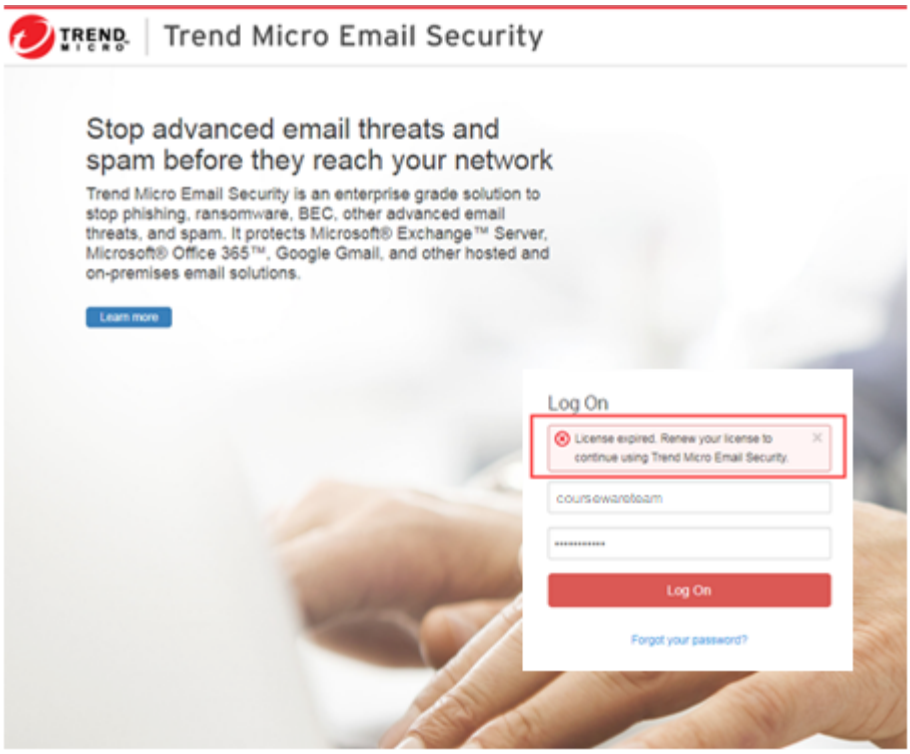


FIGURE 2.4.3.1: Freeze Period Console Interface

TIP: Disabled end user console will get this error message: **"License expired. Contact your domain administrator for details."**

FIGURE 2.4.3.2: Disabled SSO in LMP and CLP

2.4.4. Purge Period

The Purge Period is described by the table below:

Period Definition	Remind Condition	Remind Action
1. Freeze period expired 2. Calculation: Current Time is after (License expired + Grace Period + 30 days)	Starts after the end of freeze period (approximately after grace period plus 30 days)	• Purge customer's entire configurations and data permanently • Cannot be recovered

TABLE 2.4: Purge Period Summary

NOTE: Backend job runs in UTC 05:00 every day.

Chapter 3: Inbound Mail Protection

Once Trend Micro Email Security is completely provisioned, email traffic will flow according to the diagram below:

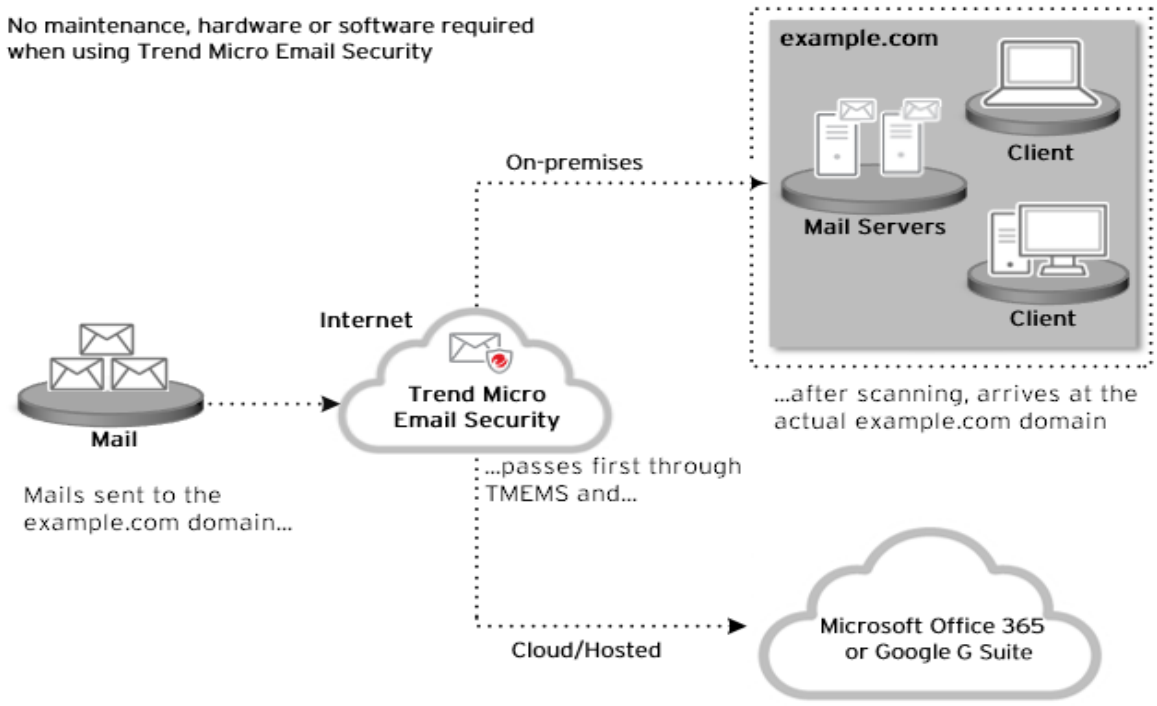


FIGURE 3.1: Inbound Mail Flow Diagram

Step Number	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 Trend Micro Email Security MTA instead of the original "example.com" Inbound Server.
2	The originating MTA routes messages to Trend Micro Email Security.
3	The Trend Micro Email Security MTA accepts the connection from the originating mail server.

TABLE 3.1: Inbound Mail Flow Process

Step Number	Description
4	Trend Micro Email Security performs IP reputation-based filtering at the MTA connection level to decide on an action to take. Actions include the following: – Trend Micro Email Security terminates the connection, rejecting the messages. – Trend Micro Email Security accepts the messages and filters them using content-based policy filtering.
5	Trend Micro 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 Trend Micro Email Security MTA routes the message to the original example.com Inbound Server.

TABLE 3.1: Inbound Mail Flow Process

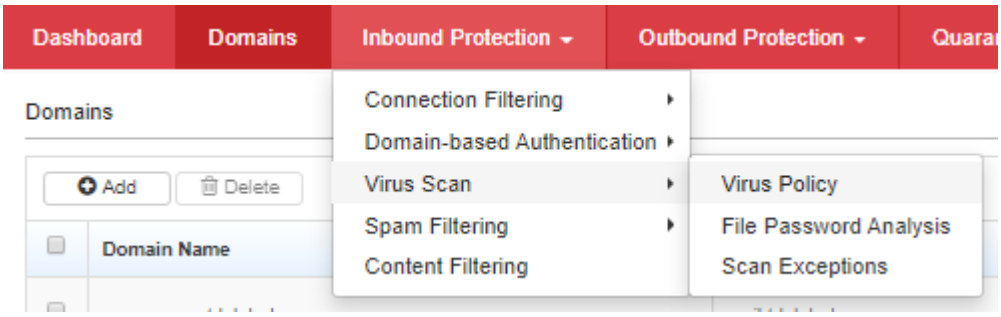
Inbound Mail Protection best practice includes enabling and configuring protection against different types of threats such as malware, spam, spoofed email messages and even ransomware.

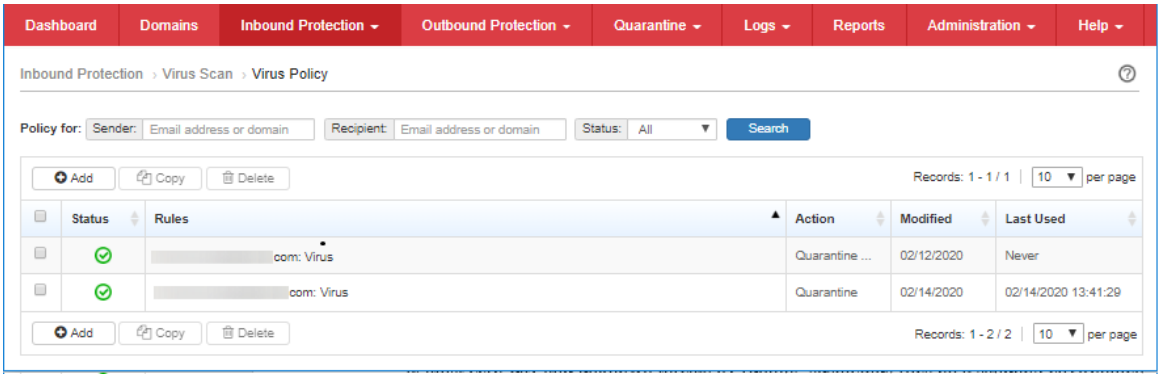
3.1. Malware and 0-Day Threats Protection

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 "Quarantine" or "Delete" action to avoid any malware to enter your environment.

1. Login to the Trend Micro Email Security administrator console.

2. Go to **Inbound Protection > Virus Scan > Virus Policy**.





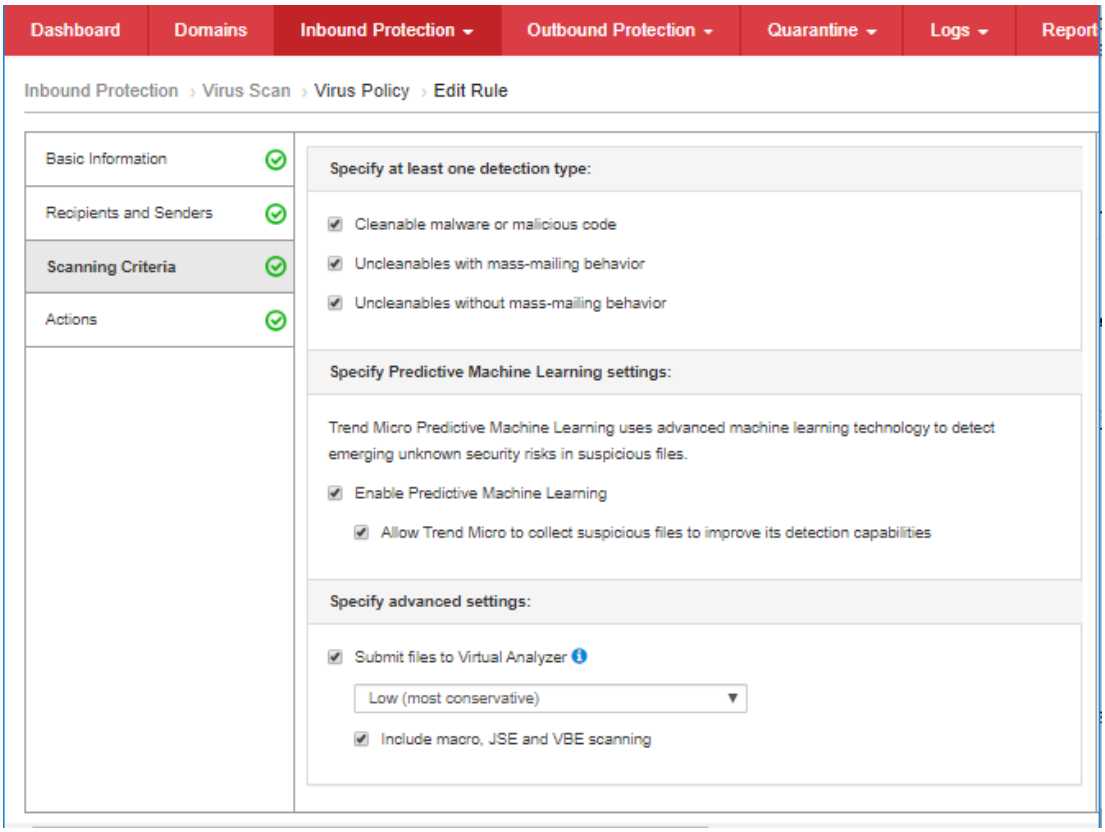
3. Make sure the action is set to **"Quarantine"** or **"Delete"**.

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

5. Under Scanning Criteria, 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.

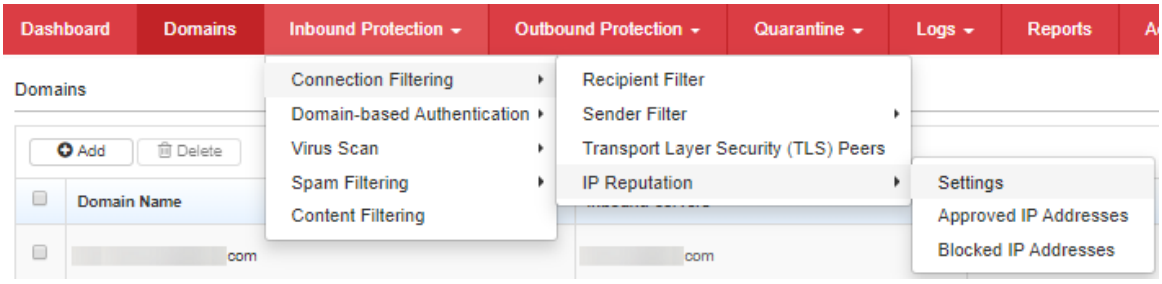
7. Enable **Predictive Machine Learning and allow Trend Micro to collect suspicious files** to improve its detection capabilities.



3.2. Spam Protection

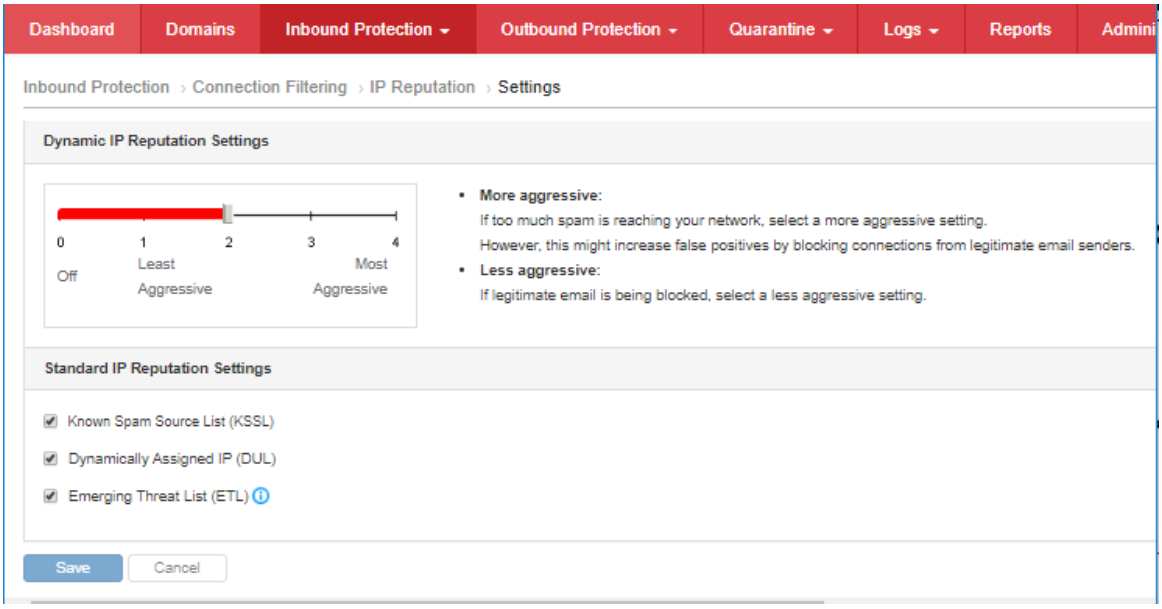
3.2.1. Configure IP Reputation setting

1. Go to **Inbound Protection > Connection Filtering > 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).

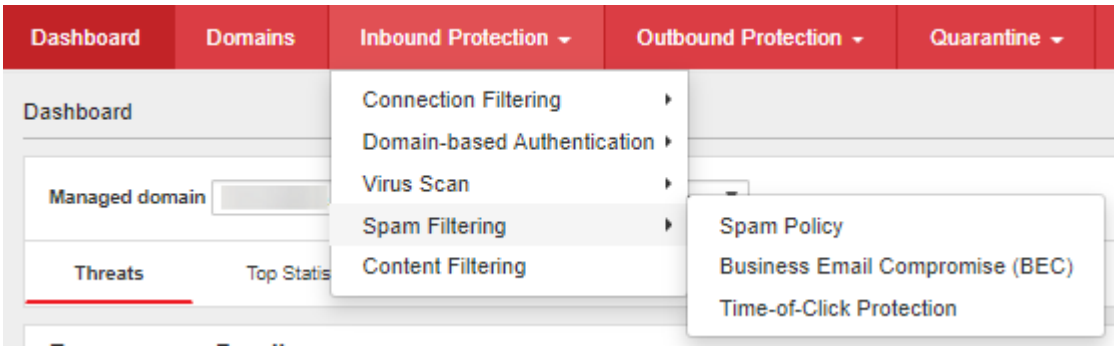


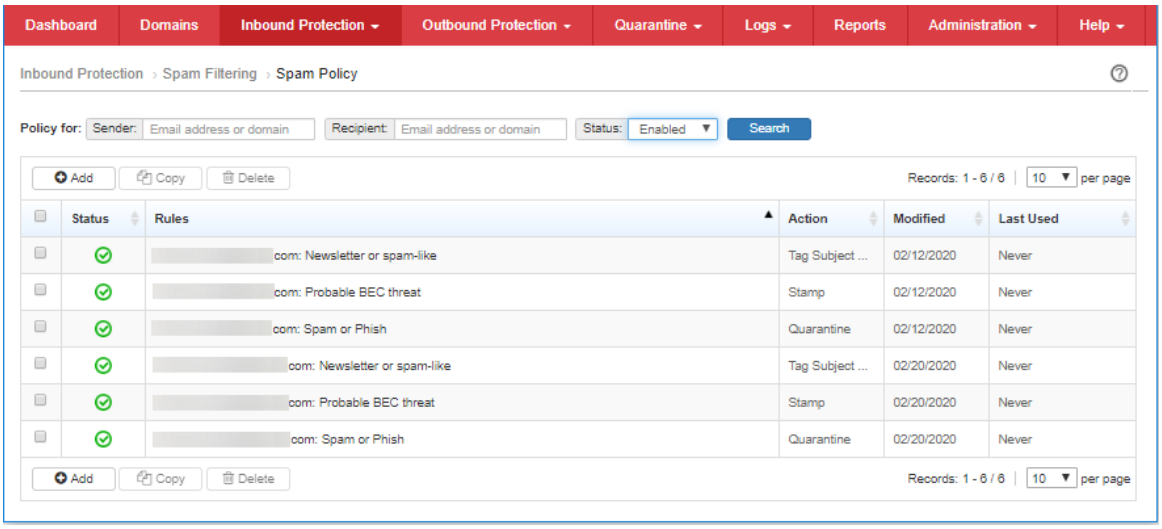
3.2.2. Add filters to default Spam or Phish policy

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. Login to the Trend Micro Email Security administrator console.

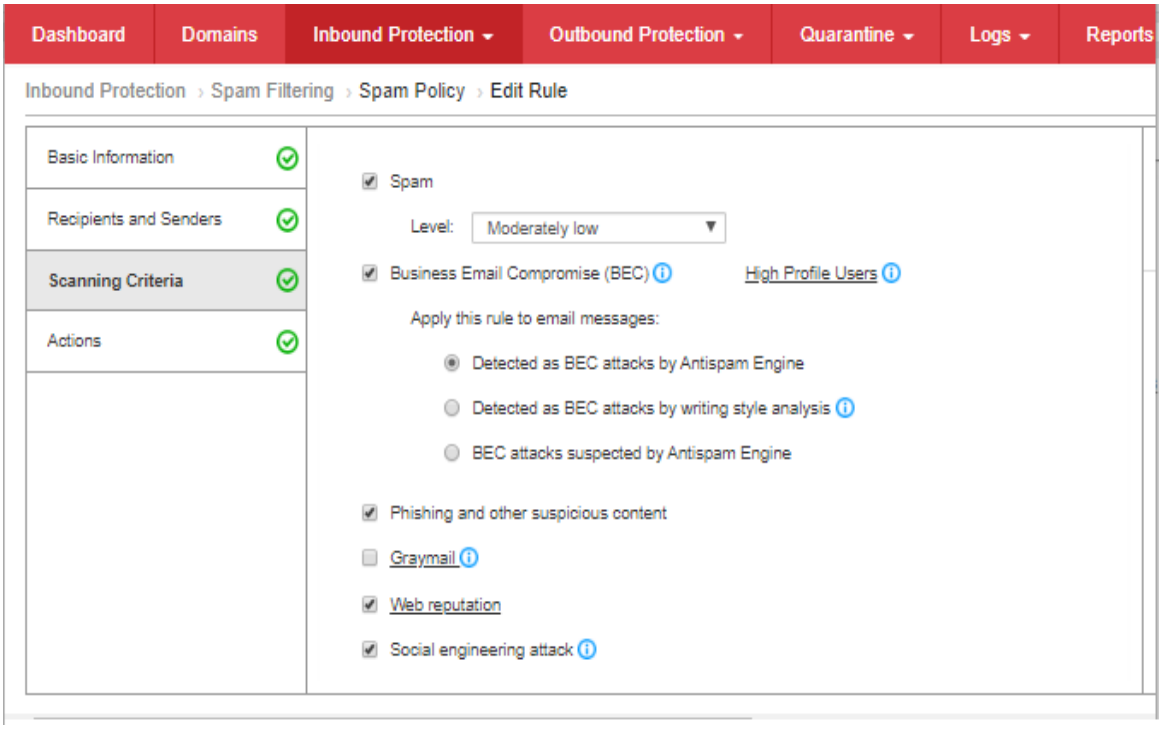
2. Go to **Inbound Protection > Spam Filtering > Spam Policy then look for the Spam or Phish policy for each managed domain**.

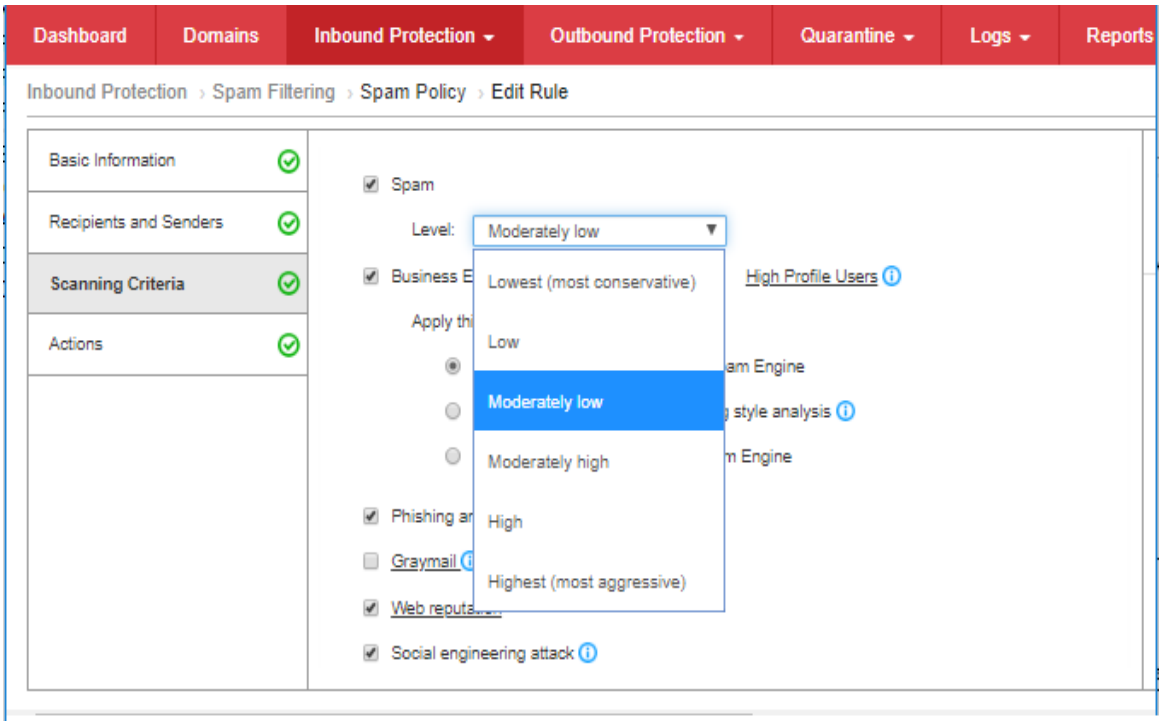




3. Click **Scanning Criteria**.

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".





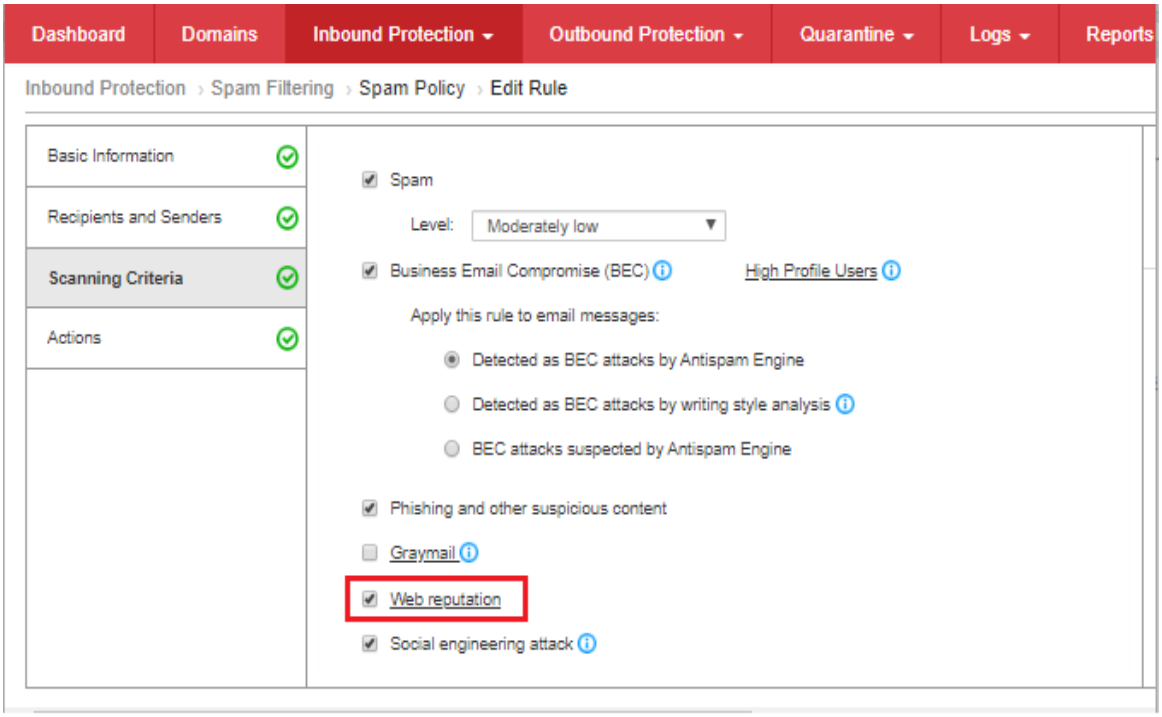
WARNING: Setting Spam check to a higher level may lead to more false positives. However, it may also reduce false negative messages and avoid malicious messages.

3.2.3. Enable Time-of-Click Protection

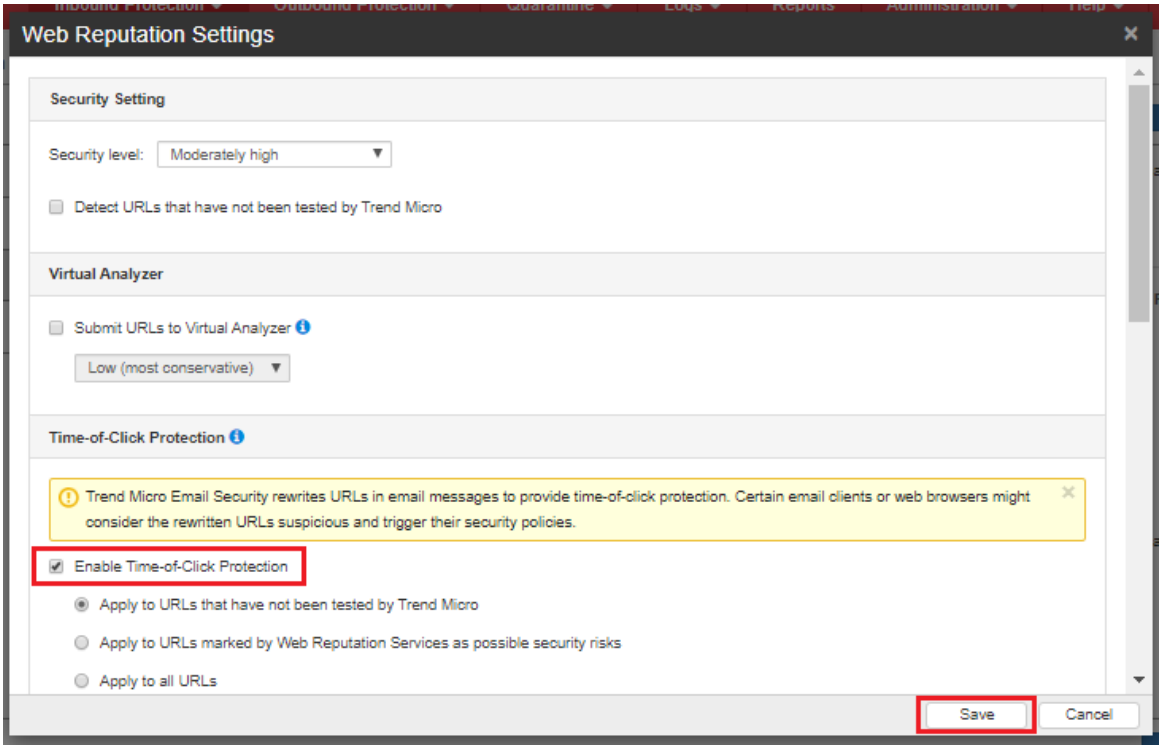
Working in conjunction with Web Reputation filter, Time-of-Click protection rewrites URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click and will block them if they are malicious to protect the users.

1. To enable Time-of-Click Protection, go to **Inbound Protection > Spam Filtering > Spam Policy > Open a specific policy or you may choose the pre-defined policy named "Spam or Phish"**.

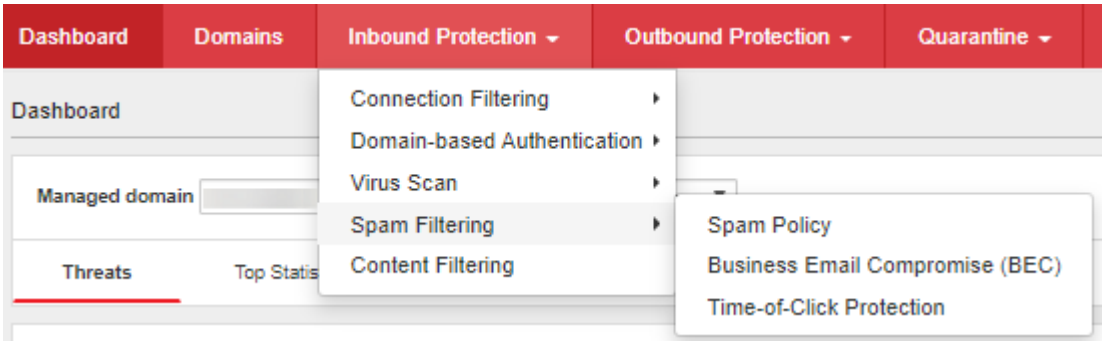
2. Click **Scanning Criteria > Web reputation**.



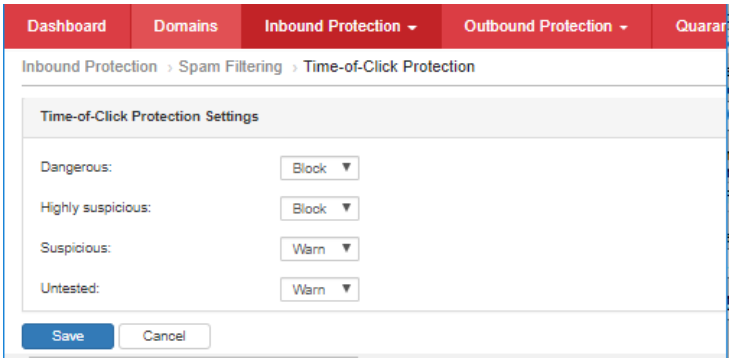
3. Click the **check box to Enable Time-of-Click Protection**. Click **Save**.



4. To configure the action when the end-user clicks the rewritten URL, go to **Inbound Protection > Spam Filtering > Time-of-Click Protection**.



5. Select the following Time-of-Click Protection Settings:



See Configuring Time-of-Click Protection Settings.

3.2.4. Enable the Newsletter or Spam-like policy

Trend Micro 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.

TIP: In order to use Graymail feature, you should use the IP reputation feature altogether.

3.3. Spoofed Email Protection

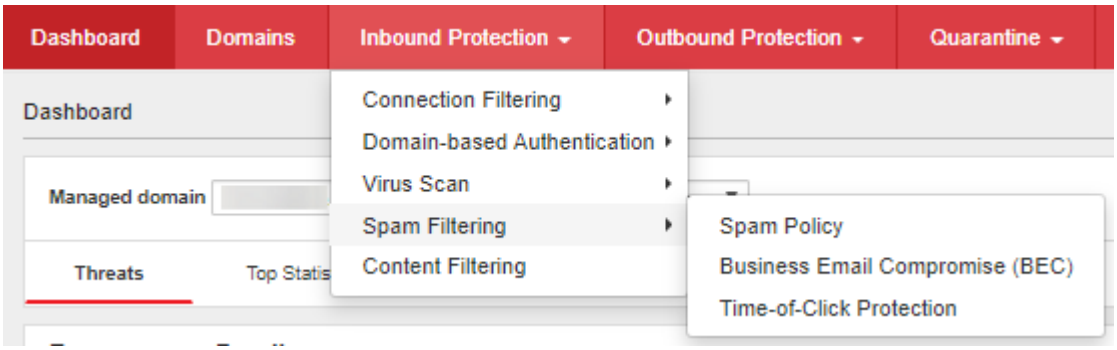
Trend Micro Email Security has multiple technologies to help protect against spoofed email messages which will be discussed in the succeeding topics.

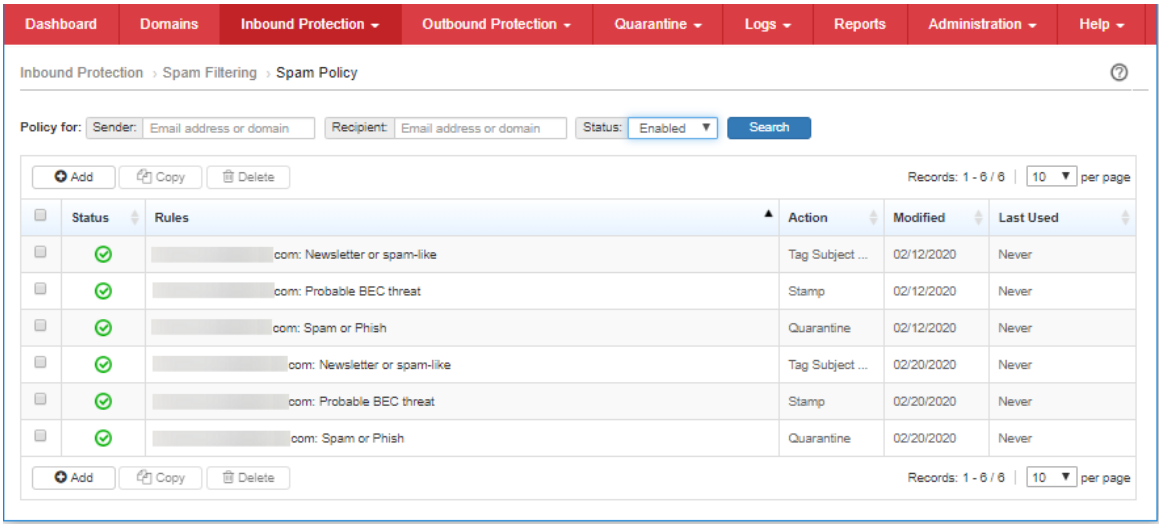
3.3.1. Enable spoofed email filters in Spam or Phish policy

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

1. Login to Trend Micro Email Security administrator console.

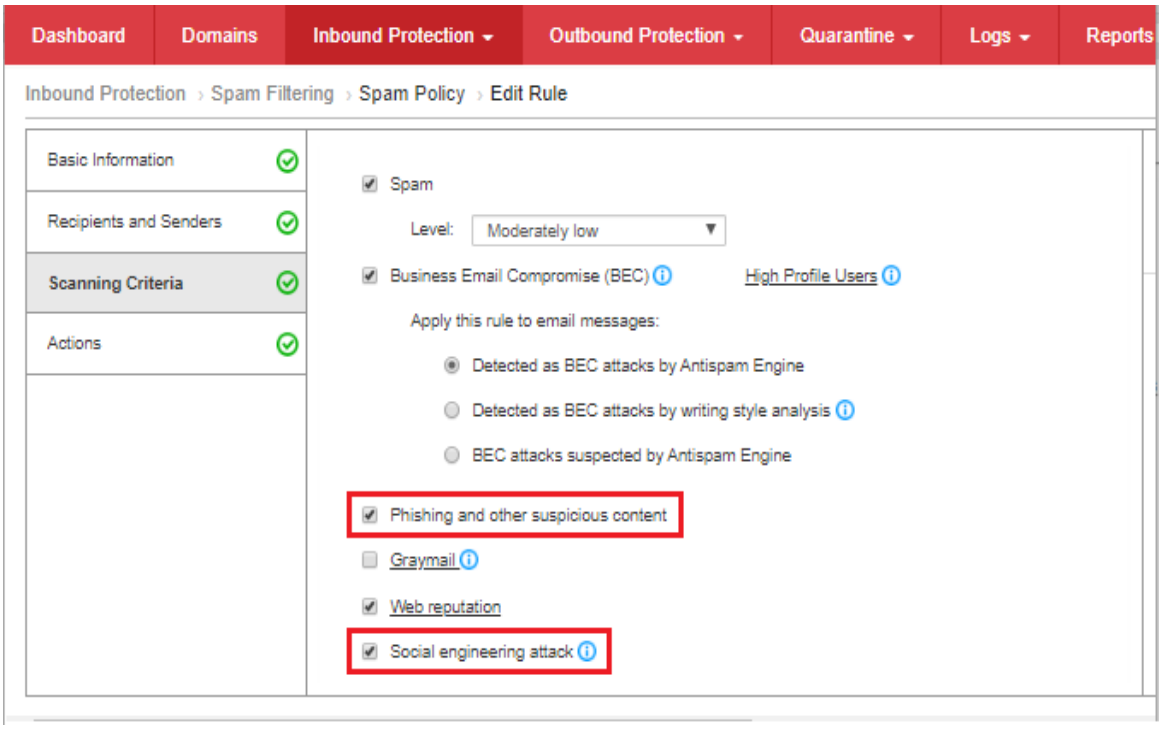
2. Go to **Inbound Protection > Spam Filtering > Spam Policy then look for the Spam or Phish policy for each managed domain**.





3. Click **Scanning Criteria**.

4. Click the **check boxes of Phishing and other suspicious content and Social engineering attack** to enable those features.



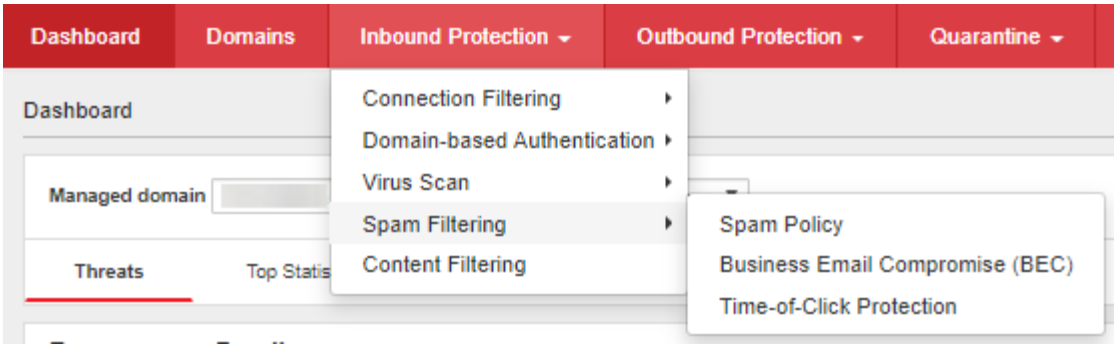
3.3.2. Configure the list of High Profile Users for Business Email Compromise filter

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 Trend Micro Email Security, it can provide tighter security for email messages claiming to be from those users.

Go to **Inbound Protection > Spam Filtering > Business Email Compromise then look for the Spam or Phish policy for each managed domain**.



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.

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 Trend Micro Email Security. Create a policy to filter email messages coming from your own domain.

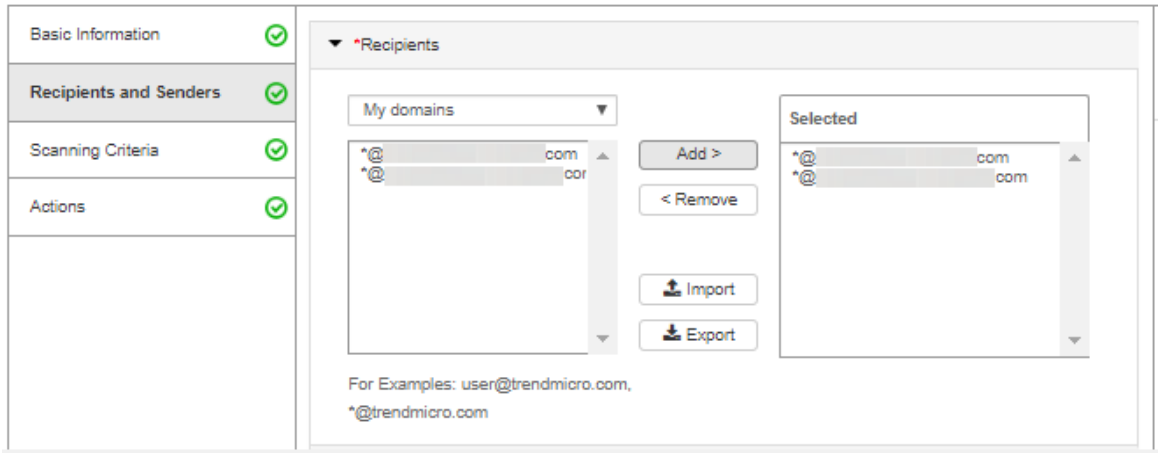
WARNING: Make sure intra-domain email messages are not routed to the Internet.

1. On your browser, login to Trend Micro Email Security administrator console.

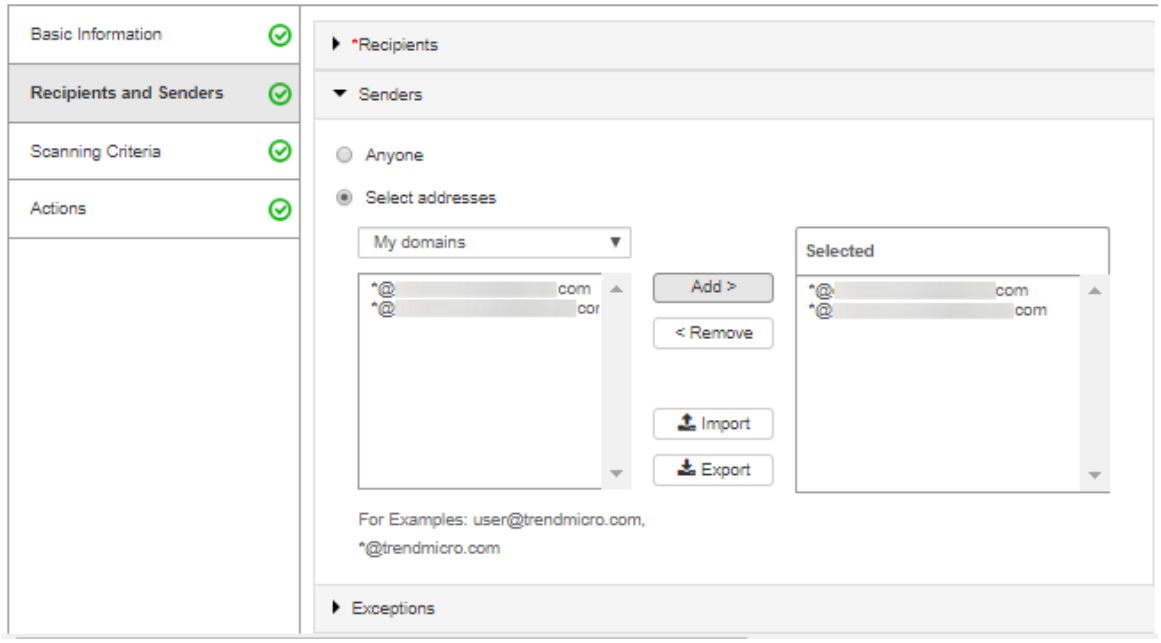
2. Go to **Inbound Protection > Content Filtering**, click **Add**.

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

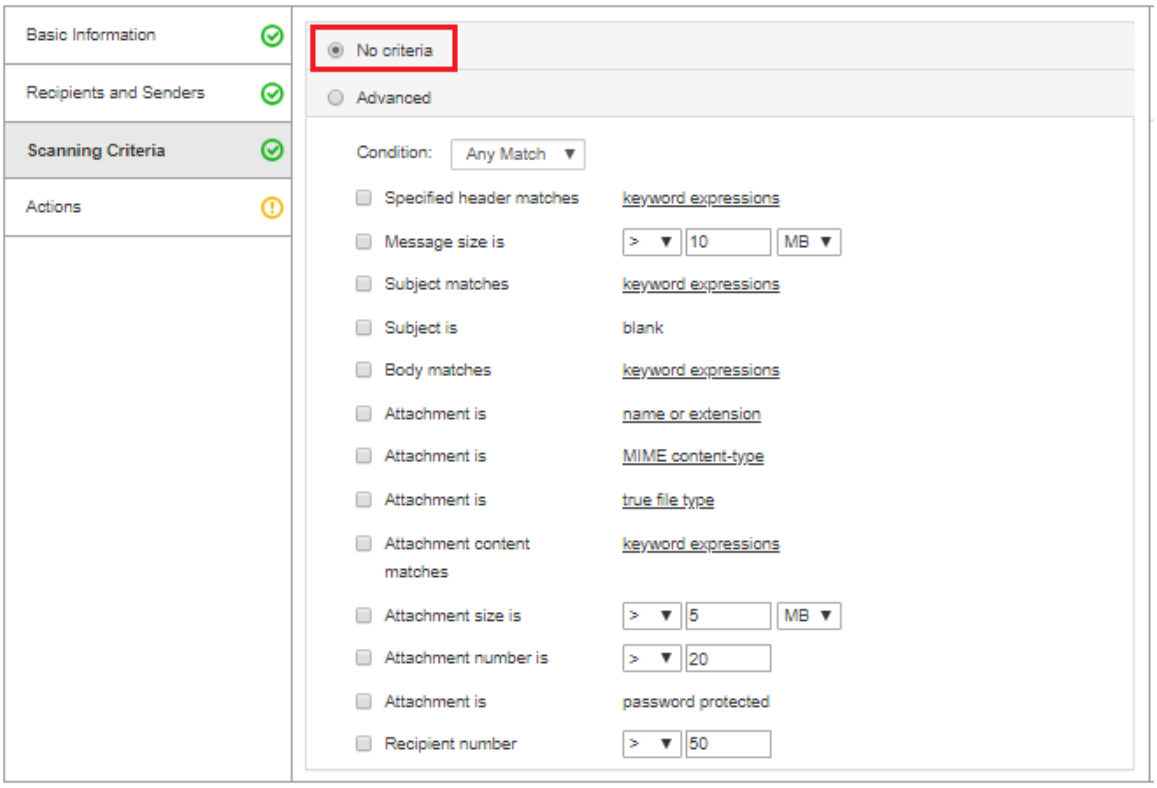
4. Go to **Recipients and Senders > Recipients**, add your domain.



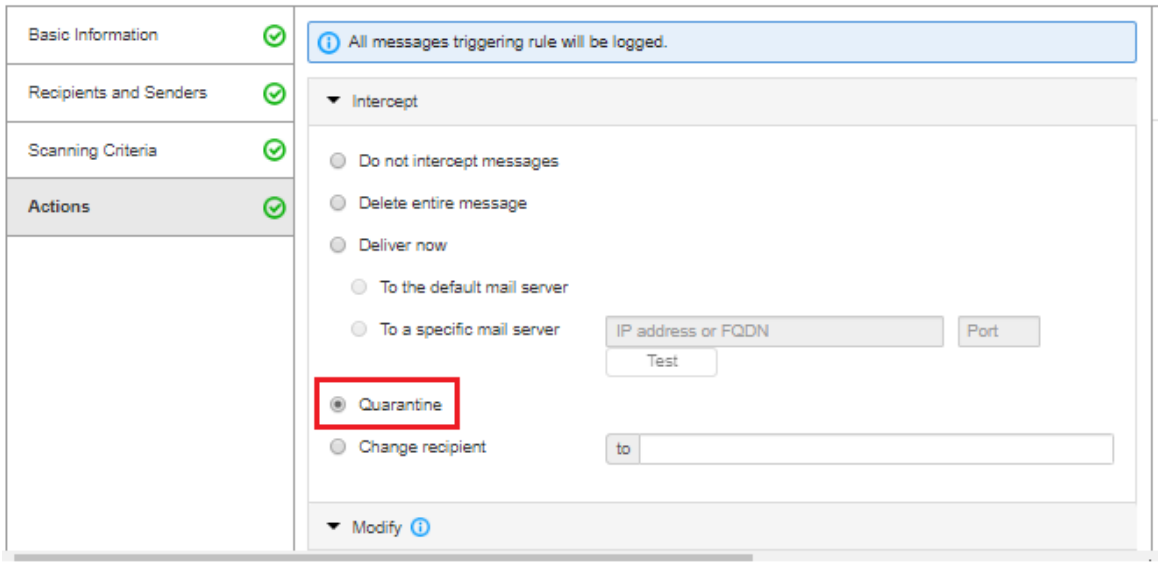
5. Go to **Recipients and Senders > Senders**, add the same domain.



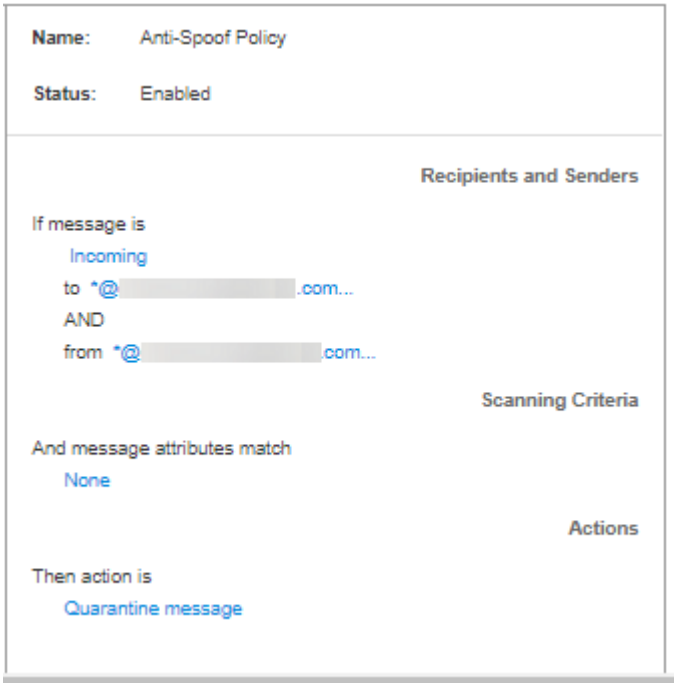
6. Under Scanning Criteria, select **No Criteria**. Any email message coming in to Trend Micro Email Security from your domain and going to your same domain will be filtered.



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



The settings will be similar below:



8. Click the **Submit** button.

3.3.4. 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. Trend Micro 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 Sender Policy Framework (SPF).

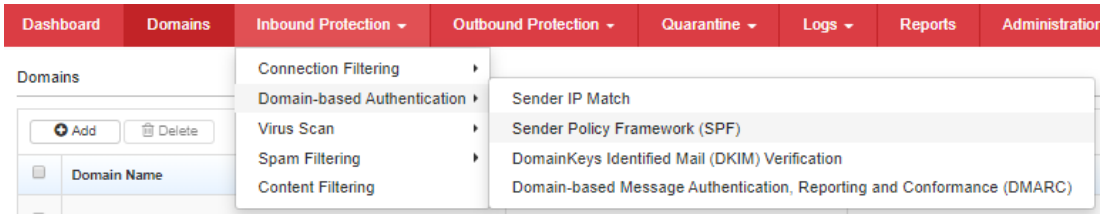
1. Enable SPF Checking in Trend Micro Email Security then create the SPF TXT record for your domain if you are using Trend Micro Email Security outbound relay.

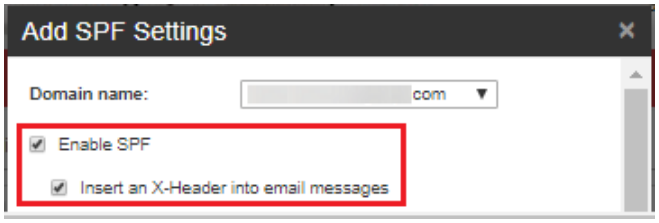
    a. Login to the administrator console.

    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"**.



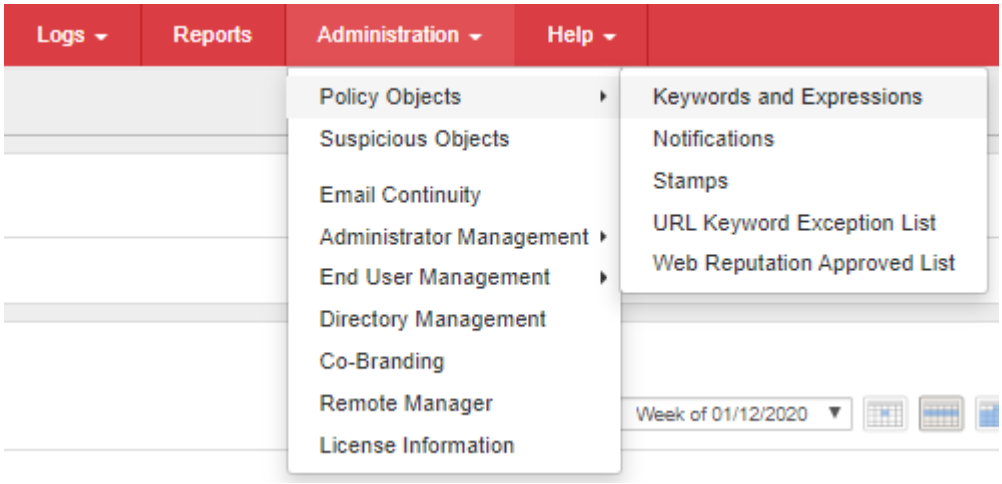


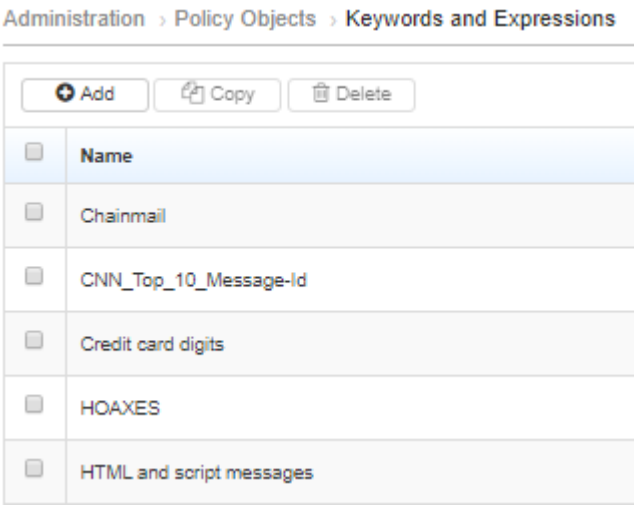
2. Create a policy to track email messages tagged by Trend Micro Email Security SPF check due to SoftFail.

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

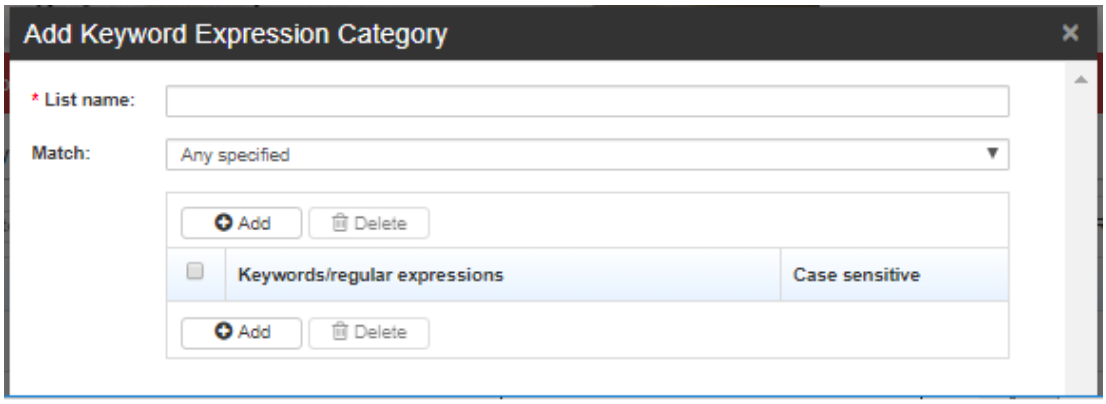
a. Login to the administrator console.

b. Go to **Administration > Policy Objects > Keywords and Expressions** and click **Add**.

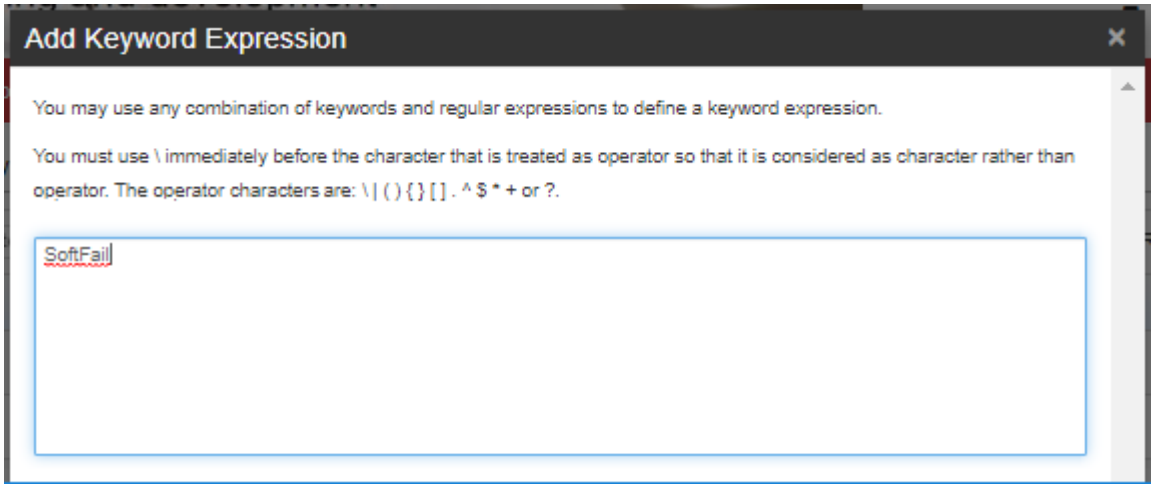




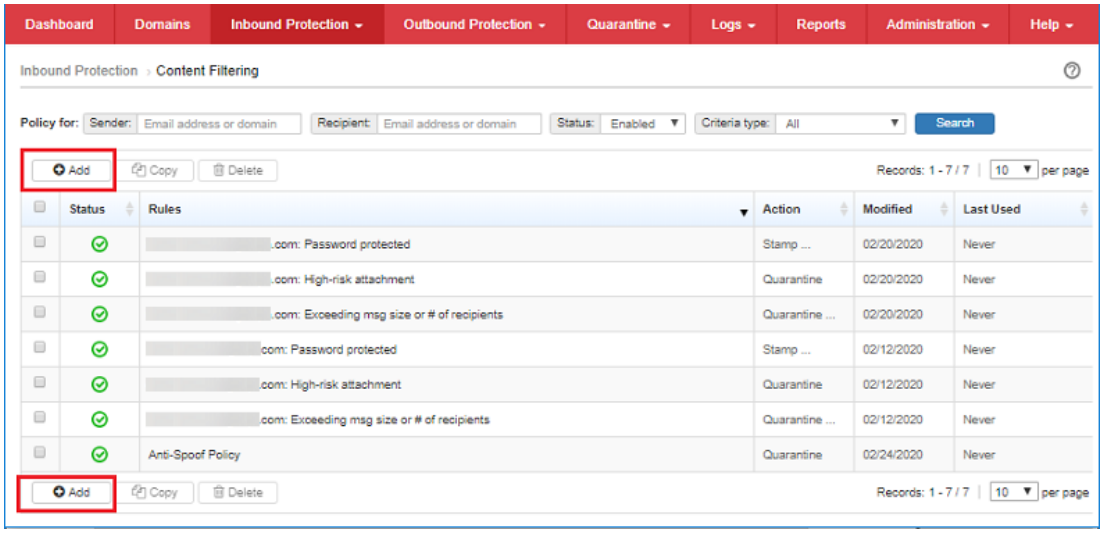
c. Type a name for the keyword list (e.g. SPF Soft Fail) then click on **Add**.



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



e. Go to **Inbound Protection > Content Filtering**, click **Add**.

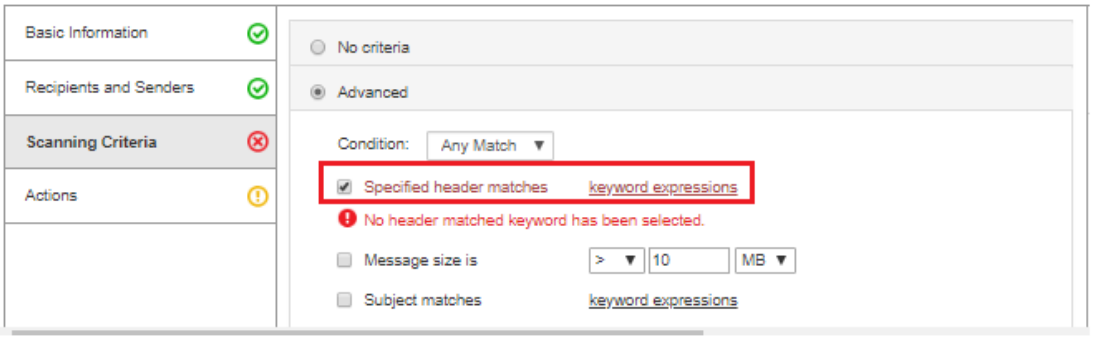


f. Under Basic Information, click the **Enable** check box then type the name of your policy (e.g. SPF check)

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

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

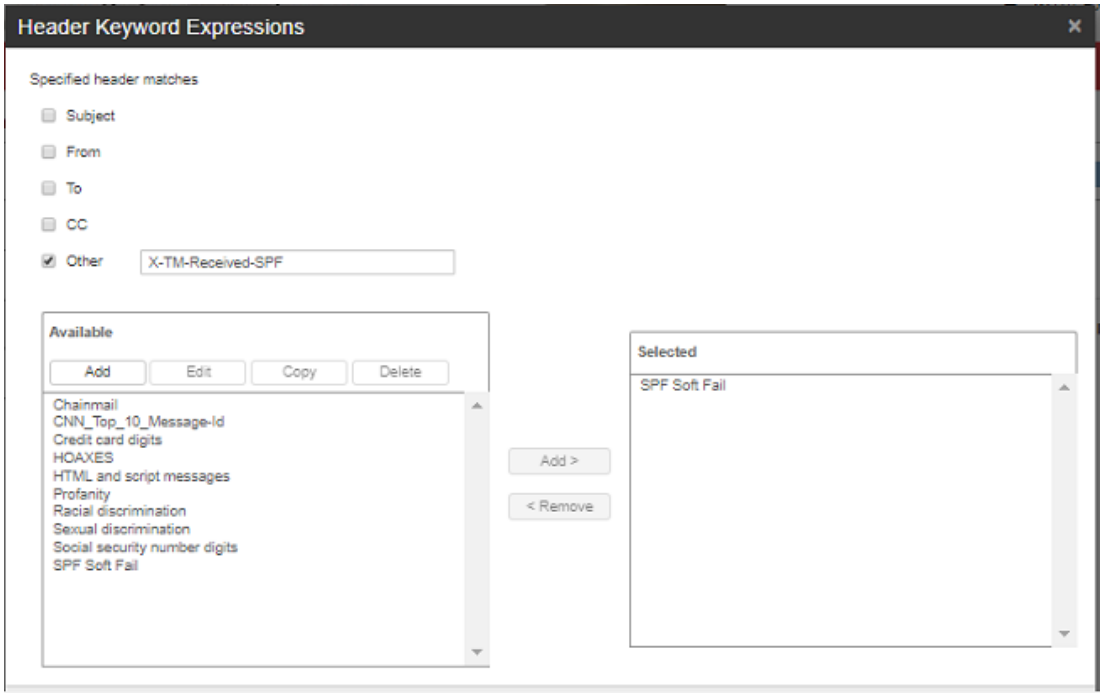
i. Click **keyword expressions** beside Specified header matches.



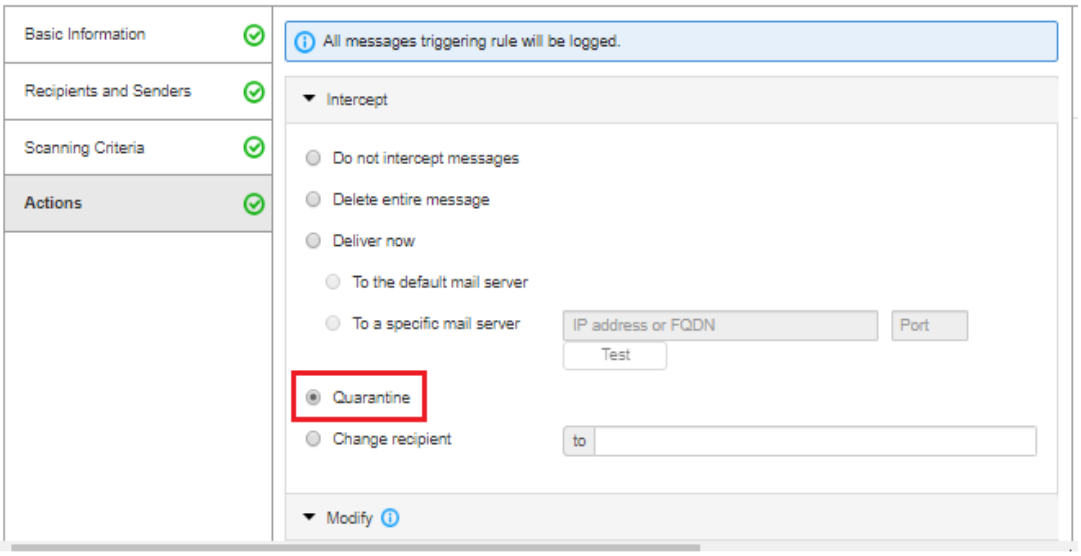
j. Check **Other** and type the keyword **"X-TM-Received-SPF"**.

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.

3.3.5. 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 within transit.

By enabling DKIM Verification, Trend Micro 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 Trend Micro Email Security, refer to 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.

3.3.6. 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 Trend Micro 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.

Click this link for more information about Domain-based Message Authentication, Reporting & Conformance (DMARC).

To enable DMARC:

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.

3.4. Approved and Blocked Sender

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.

3.4.1. Approved Sender

1. Minimize the amount of addresses in the **Inbound Protection > Connection Filtering > 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.

3.4.2. Blocked Sender

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

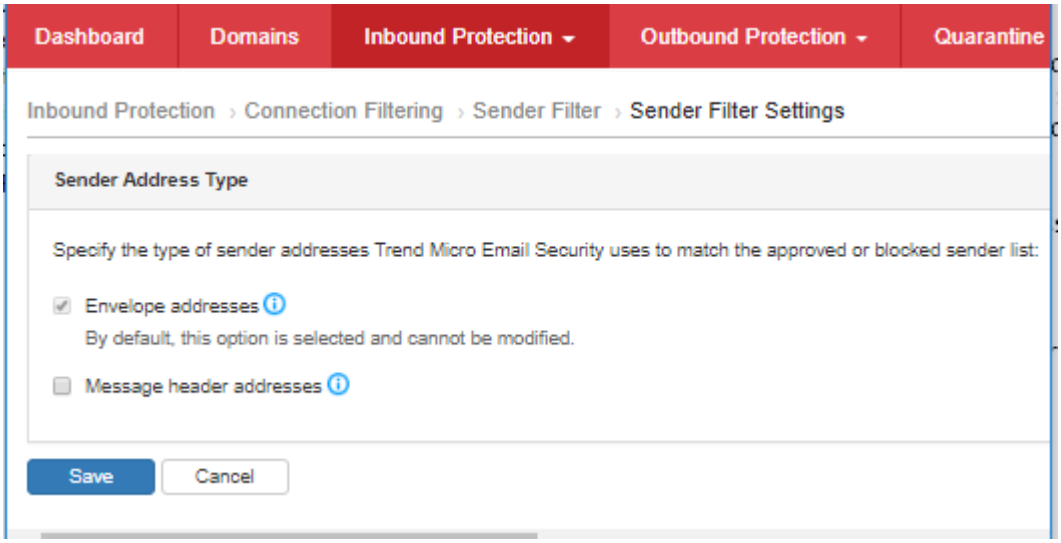
2. If no internal email message passes through Trend Micro Email Security, internal domains may be added in the Blocked Senders list to protect against envelope sender spoofing.

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

3.5. 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 > Connection Filtering > Sender Filter > Sender Filter Settings**.

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



For more details, refer to Sender Address Types.

3.6. Backscatter Spam and Directory Harvest Attacks (DHA) email messages

Trend Micro Email Security uses user directories to help prevent backscatter (or outscatter) spam and Directory Harvest Attacks (DHA). Importing user directories lets Trend Micro 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 Directories

See Directory Management.

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

1. Go to **Inbound Protection > Connection Filtering > 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.

3.7. Incoming Transport Layer Security

Transport Layer Security (TLS) is a protocol that helps to secure data and ensure communication privacy between endpoints. Trend Micro Email Security allows you to configure TLS encryption policies between TMEMS and specified TLS peers.

TIP: Trend Micro 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 > Connection Filtering > Transport Layer Security (TLS) Peers** of the administrator console, Trend Micro 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 Trend Micro 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 Trend Micro Email Security administrator console, go to **Inbound Protection > Connection Filtering > 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, refer to Transport Layer Security (TLS) Peers.

3.8. 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.

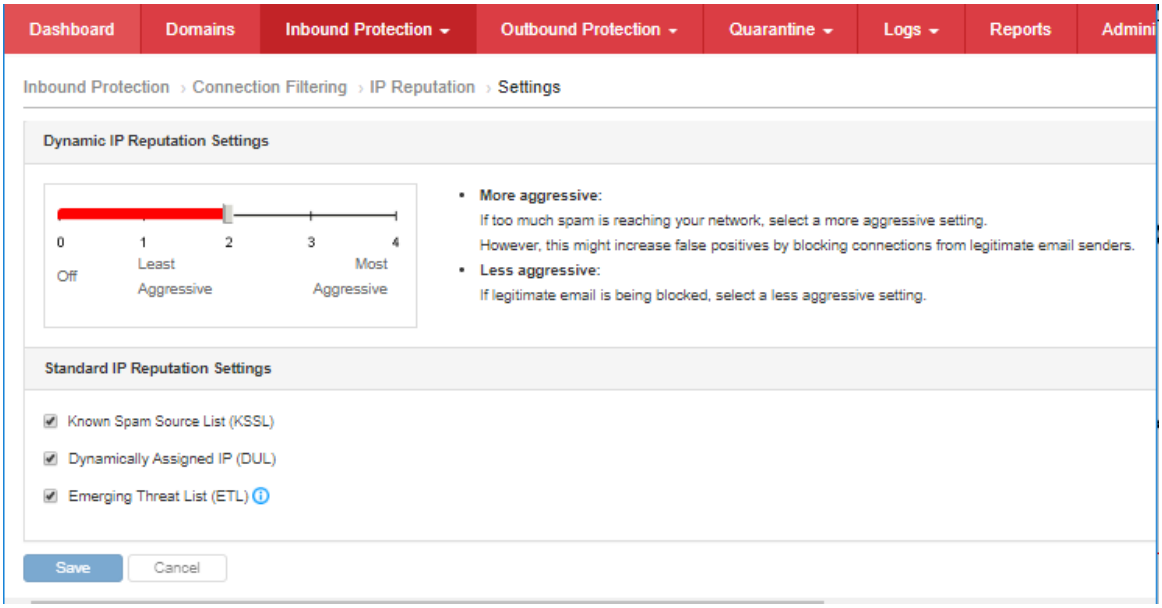
To increase protection from Ransomware threats in Trend Micro Email Security, follow the topics below:

3.8.1. Enable IP Reputation setting

1. Go to **administrator console > Inbound Protection > Connection Filtering > IP Reputation > Settings**.

2. Use the Dynamic IP Reputation Settings slider to adjust how aggressively Email Reputation Services (ERS) blocks email connections. Below are blocking levels:

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



We recommend that you make changes to the Dynamic Settings carefully and in small increments. You can then update your settings based on the increased amount of spam and legitimate messages received.

For more details, refer to About Dynamic IP Reputation Settings.

3.8.2. Ensure that Spam and Phish inbound policy is enabled

1. Go to **administrator console > Inbound Protection > Spam Filtering > Spam Policy**.

2. Open Spam or Phish policy for each managed domain.

3. Review the settings enabled under Scanning Criteria if enabled (e.g. Spam, Phishing and other suspicious content, Web reputation, etc.).

3.8.3. Block file types commonly used by Ransomware

The Attachment True File Type criteria allows you to create rules that take actions on messages based on the true file type of attachments inside the email.

1. Go to **administrator console > Inbound Protection > Content Filtering, click Add**.

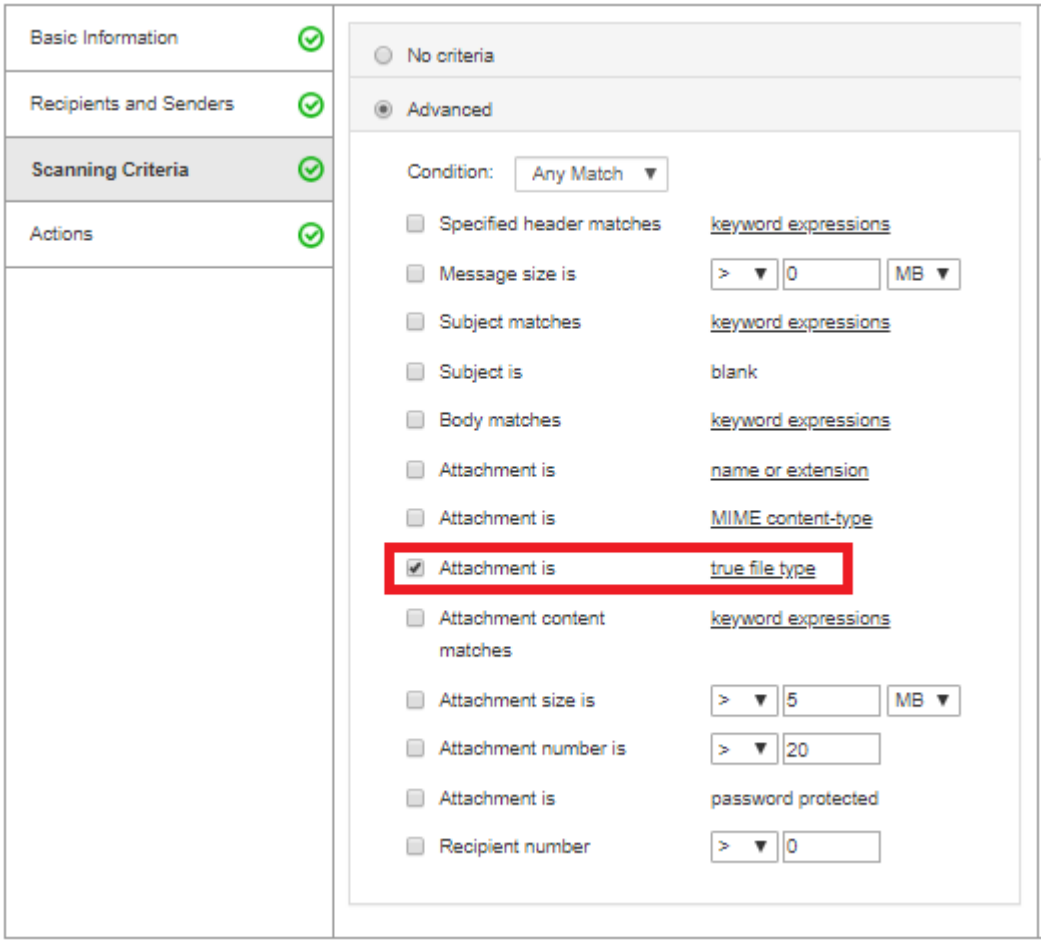
2. Type name of the rule you are creating (e.g. BLOCK_EXE). Make sure **Enable** check box is selected.

3. Go to **Recipients and Senders > Recipients**, add your domain. There is an option to define Recipient Exceptions. Use it carefully according to organizational needs.

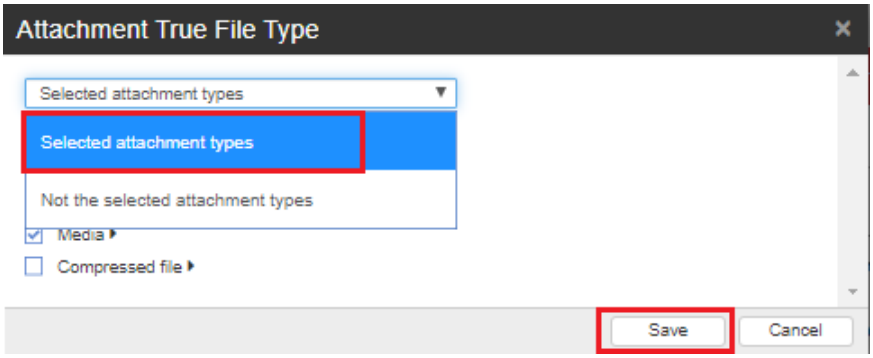
4. Go to **Recipients and Senders > Senders**, the default is Anyone. Under Select addresses, you can choose to input address or domain. There is an option to define Sender Exceptions but use it carefully according to organizational needs.

5. Under Scanning Criteria, select **Advanced**.

6. Select the **"Attachment is"** check box then click **true file type**.



7. Under Attachment True File Type, on the drop down list, choose **"Selected attachment types"**.



8. Select the true file types (exe, etc.) to match on. Click **Save**.

9. Under Actions, select **"Quarantine"** in order to still review filtered email messages with matching attachment such as .exe file.

10. Click **Submit**.

For more information on other file types recommended to be blocked at the email gateway, refer to Knowledge Base Article 1122150.

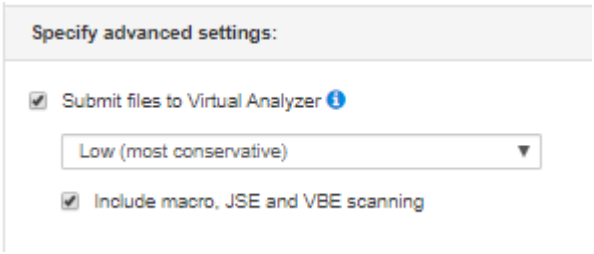
3.8.4. Enable macro file scanning

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

1. Login to Trend Micro Email Security administrator console.

2. Go to **Inbound Protection > Virus Scan > Virus Policy and select Virus rule**.

3. Go to **Scanning Criteria > Specify advanced settings**, select **Enable Virtual Analyzer.** Afterwards, select **Include macro, JSE and VBE scanning**.



4. Click **Submit**.

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

3.9. Sender IP Match

With Sender IP Match, Trend Micro Email Security enables you to specify an IP address or a range of addresses within a domain and allow email messages only from those addresses of the specified domain. Sender IP Match is a way that readily allows you to simultaneously approve all inbound email traffic from a particular domain while equally preventing spoofing by manually defining the allowed IP ranges.

If an email message passes the Sender IP Match check, Trend Micro Email Security skips its own SPF checking as well as the SPF checking of DMARC authentication for this message.

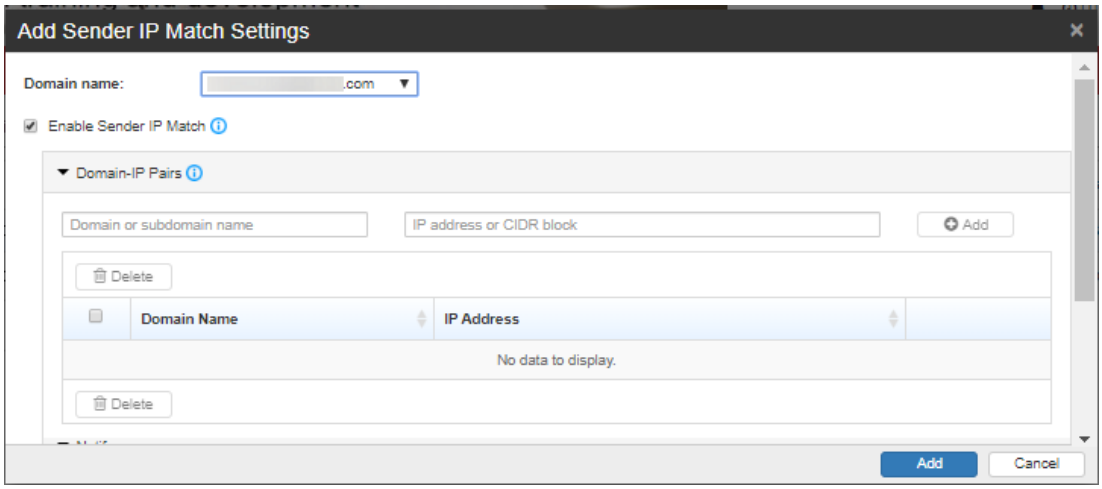
1. Go to **Inbound Protection > Domain-based Authentication > Sender IP Match**.

2. Click **Add**. The Add Sender IP Match Settings screen appears.

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

4. Select **Enable Sender IP Match**.

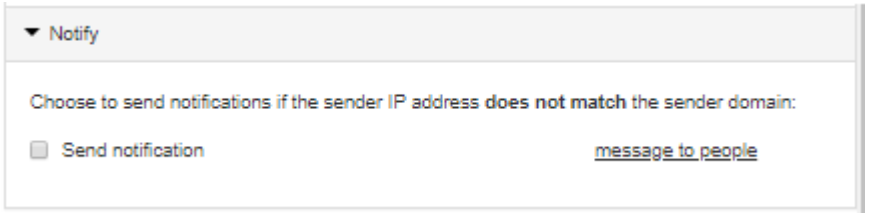
5. Under Domain-IP Pairs, add one or multiple domain-IP pairs.
   a. Specify a sender domain using one of the following formats:
      - example.com
      - subdomain.example.com
      - *.example.com
   b. Specify one or multiple IP addresses or IP blocks to pair with the domain.
   c. Click **Add**.



6. Under Intercept, specify the action to take if the sender IP address does not match the sender domain as you specified.

7. Under Notify, select to **Send notification** option then choose at least one notification template.

8. Click **Add**.



For more details, refer to Sender IP Match.

3.10. File Password Analysis

By leveraging a combination of user-defined passwords and message content (subject, body and attachment names), Trend Micro Email Security can heuristically extract or open password-protected files, namely, archive files and document files. This is to detect any malicious payload that may be embedded in those files.

You can add or import user-defined passwords to help Trend Micro Email Security efficiently extract or open password-protected files for further scanning.

Trend Micro Email Security supports the following password-protected archive file types:

- 7z
- rar
- zip

Trend Micro Email Security also supports the following password-protected document file types:

- doc
- docx
- pdf
- pptx
- xls
- xlsx

Below are the steps on how to configure File Password Analysis:

1. Choose **Inbound Protection > Virus Scan > File Password Analysis**.

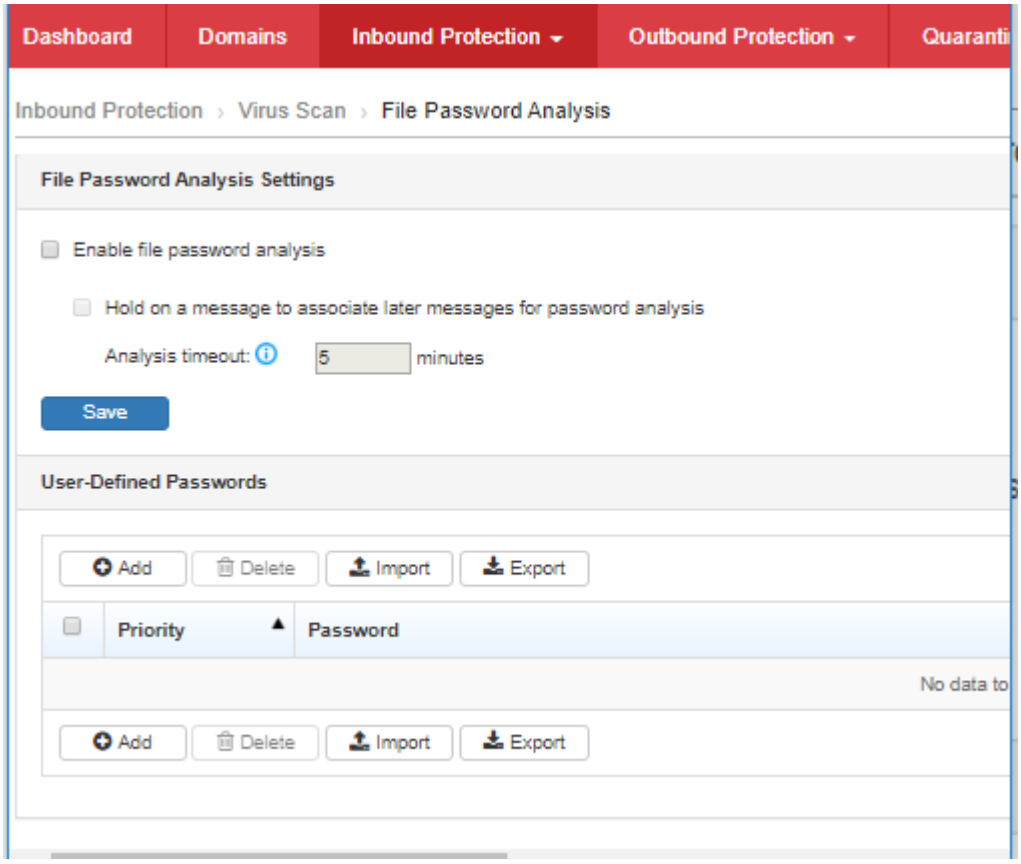
2. In the File Password Analysis Settings section, select **Enable file password analysis**.

3. Optionally select **Hold on a message to associate later messages for password analysis** and specify a certain amount of time for Analysis timeout.

NOTE: This step is required if you want Trend Micro Email Security to associate later email messages to further analyze the file password for the current email message. The current message will not be released for delivery during the analysis timeout period.

4. Click **Save**.

TIP: To help Trend Micro Email Security crack file passwords more efficiently, you can add or import passwords that are commonly used by your organization as the user-defined passwords. Trend Micro Email Security will try the user-defined passwords first before any other ways to extract or open files.



For more details, refer to File Password Analysis.

Chapter 4: Outbound Mail Protection

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

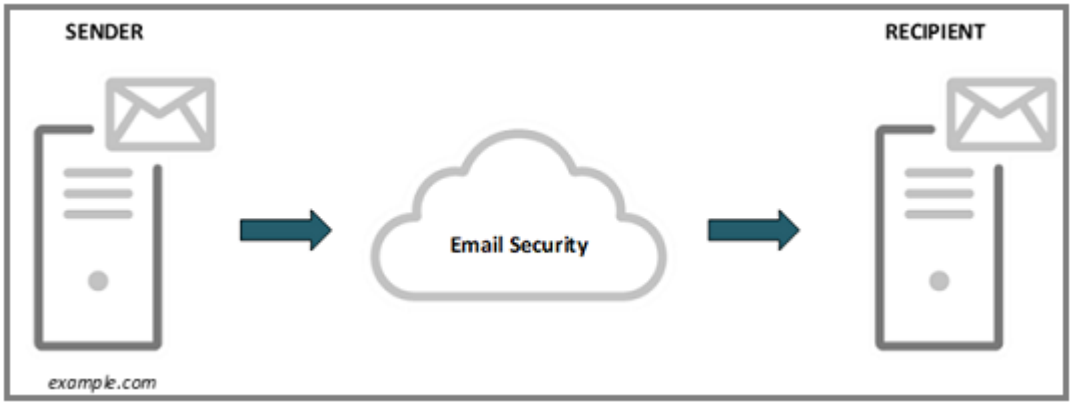


FIGURE 4.1: Outbound Mail Flow Diagram

Step Number	Description
1	Mail server of example.com will forward the outbound email message to Trend Micro Email Security.
2	Trend Micro 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

4.1. Policies

Trend Micro Email Security has separate policies applied to outbound email messages. Depending on organizational needs, these policies may be adjusted to meet specific requirements.

4.1.1. Outbound Virus policy

By default, Trend Micro Email Security has a Global Outbound Policy – Virus policy. This policy scans for possible malicious files that may come from your network.

The default action is "Quarantine". This policy is enabled to protect your organization from possible damage reputation due to malware spread. This policy can be found in the **administrator console > Outbound Protection > Virus Scan > Virus Policy > Global Outbound Policy (Virus)**.

NOTE: This policy cannot be edited, but you can create another Virus Policy.

4.1.2. Add additional outbound Spam and Phish policy

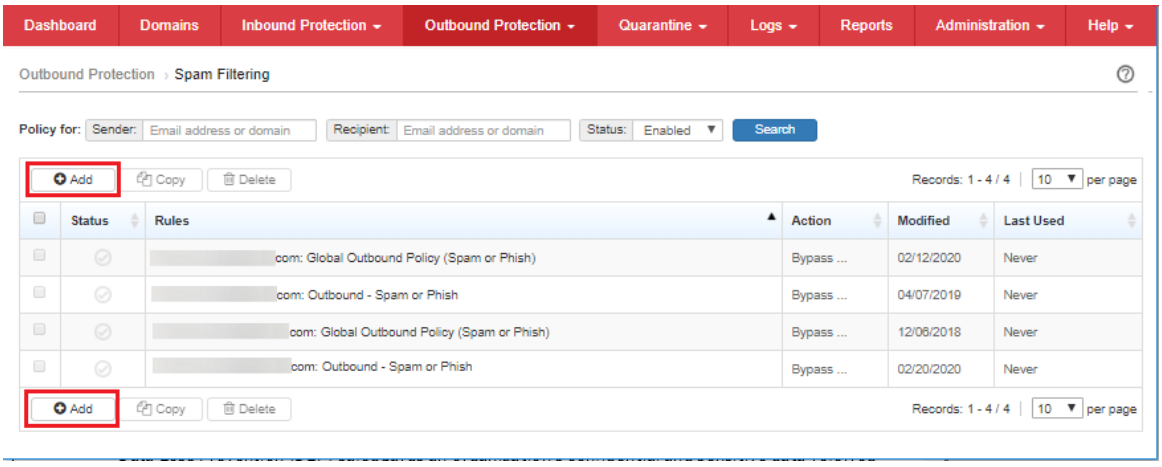
Trend Micro Email Security Global Outbound Policy (Spam or Phish) is a default rule to avoid outbound spam and prevent Trend Micro Email Security outbound servers from being blocked by 3rd party Known Spam Source List (KSSL). The policy cannot be edited and they are activated by default for all domains.

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 Trend Micro Email Security administrator console.

2. Go to **Outbound Protection > Spam Filtering** 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**.

4.1.3. Data Loss Prevention policy

Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data-referred to as digital assets against accidental disclosure and intentional theft.

Data Loss Prevention allows you to:
- Identify the digital assets to protect
- Create policies that limit or prevent the transmission of digital assets through email
- Enforce compliance to established privacy standards

DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission.

4.2. Outgoing Transport Layer Security

Similar to Incoming Transport Layer Security (TLS), Trend Micro Email Security also has a default policy that enables Opportunistic TLS for all outgoing connections.

This includes connections from Trend Micro 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. Trend Micro Email Security will use TLS when sending email messages to these domains.

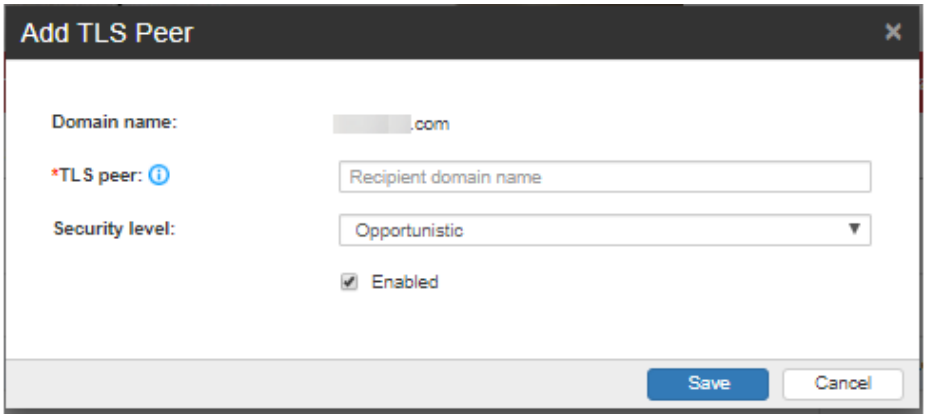
1. From Email Security administrator console, go to **Outbound Protection > Transport Layer Security (TLS) Peers**.

2. Click **Add**.

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

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

5. Click **Save**.



4.3. Publish SPF record in DNS

When using Outbound Filtering in Trend Micro Email Security, your outbound mails will be routed to Trend Micro Email Security first.

Trend Micro Email Security will relay it to the destination domains. Given this, you can add Trend Micro Email Security outbound IP addresses in your domain's SPF record to let recipients know that your outbound mails should only come from Trend Micro Email Security.

When using Trend Micro Email Security outbound scanning, the following is the recommended SPF record: **v=spf1 include:spf.tmes.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.

4.4. 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 Trend Micro Email Security outbound filtering. Below are the steps:

1. Go to **Outbound Protection > 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. Trend Micro 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/
MkWAU1VHD39bUVByu0dlmQdEodBqcPxyev/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:

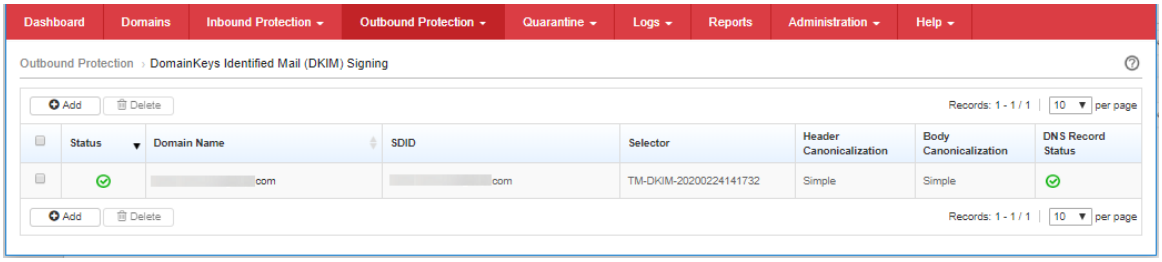
TM-DKIM-201705241492 3._domainkey	**IN**	**TXT**	**"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEF AAOCAQ8AMIIBCgKCAQEA5m HBjC/ WCkQ5WRWJ4Ln64EssFPQojX0y NIOTgjrchcK0/ IKX1eRvZzbX8kErmgT5hvEys9tD oW7iG/ zAZUqhmtgDuha8ULFknxsvrMhPs Vs3jSjX373bBWtOgI+izFCH+MU6 KznyJZGcckEsPkS3ffy"**
TM-DKIM-2017052414923._domainkey	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.

   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.



4.5. Email Encryption

Trend Micro 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.

Trend Micro Email Security does not automatically encrypt email messages. When outbound filtering is enabled, outbound encryption appears as a rule option within the Trend Micro Email Security administrator console. You need to configure rules to apply encryption as a rule action.

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

1. From the Trend Micro Email Security administrator console, go to **Outbound Protection > Content Filtering**.

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: End User Management

End User Management provides a way for customers using Active Directory to enable single sign-on for End User Console (EUC) access.

By enabling and configuring this feature, end users will not need to manage and memorize an additional account name and password for EUC. Instead, they will use their own Active Directory credentials to login to EUC console.

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

Refer to the Configuring Single Sign-On for the complete details on how to configure this feature.

There is an option to use Local Account Logon wherein end users can log on to the End User Console with their username and password. The credentials will be from local managed accounts that they have registered on the End User Console.

For more details, refer to End User Management.

5.1. End User Console

End User Console (EUC) is a separate independent console where end users can login and manage their quarantined mails by Trend Micro Email Security. Below are the ways on how to access End User Console:

Logon Method	Logon Information
Single sign-on (SSO)	If your administrator has enabled SSO, ask your administrator for the logon address then log on to the End User Console with your identity provider credentials.
Local account logon	Use the following web address for your region to access the End User Console: • North America, Latin America and Asia Pacific: https://euc.tmes.trendmicro.com • Europe, the Middle East and Africa: https://euc.tmes.trendmicro.eu • Australia and New Zealand: https://euc.tmes-anz.trendmicro.com • Japan: https://tm.tmems-jp.trendmicro.com **NOTE:** For detailed operations on the local accounts, see Local Account Management.

TABLE 5.1: End User Console Login Method Summary

For more details, refer to Getting Started with the End User Console.

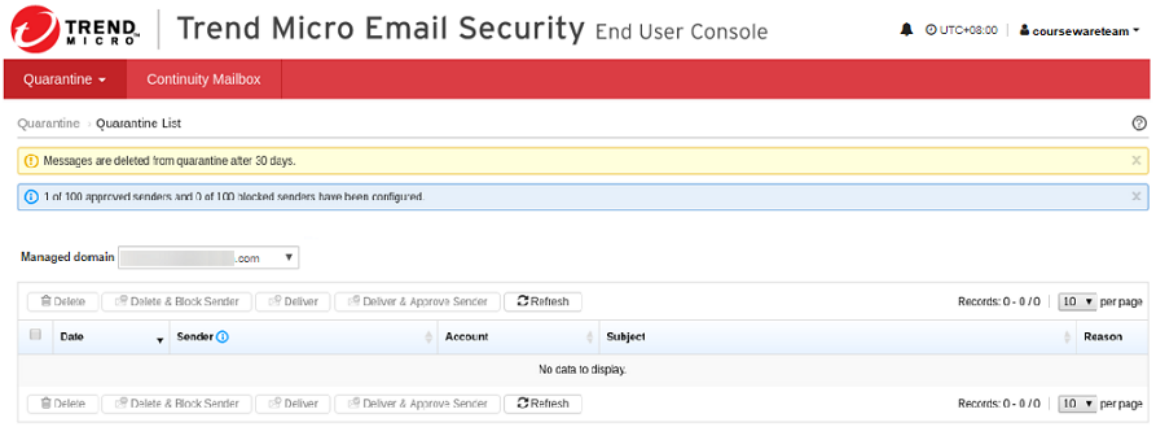


FIGURE 5.1: End User Console Quarantine List

5.2. Digest Setting and Digest Mail

The Quarantine Digest lists up to 100 of each end user's quarantined email messages. It provides a link for that account holder to access quarantined messages through the End User Console at the following web address for your region:

- North America, Latin America and Asia Pacific: https://euc.tmes.trendmicro.com
- Europe, the Middle East and Africa: https://euc.tmes.trendmicro.eu
- Australia and New Zealand: https://euc.tmes-anz.trendmicro.com
- Japan: https://tm.tmems-jp.trendmicro.com

Use the Digest Settings screen (**Quarantine > Digest Settings**) to configure the schedule and format for the Quarantine Digest.

If Quarantine Digest is enabled, all domain recipients will receive their own customized copy of the digest. Intended message recipients can use the End User Console to manage quarantined messages by themselves.

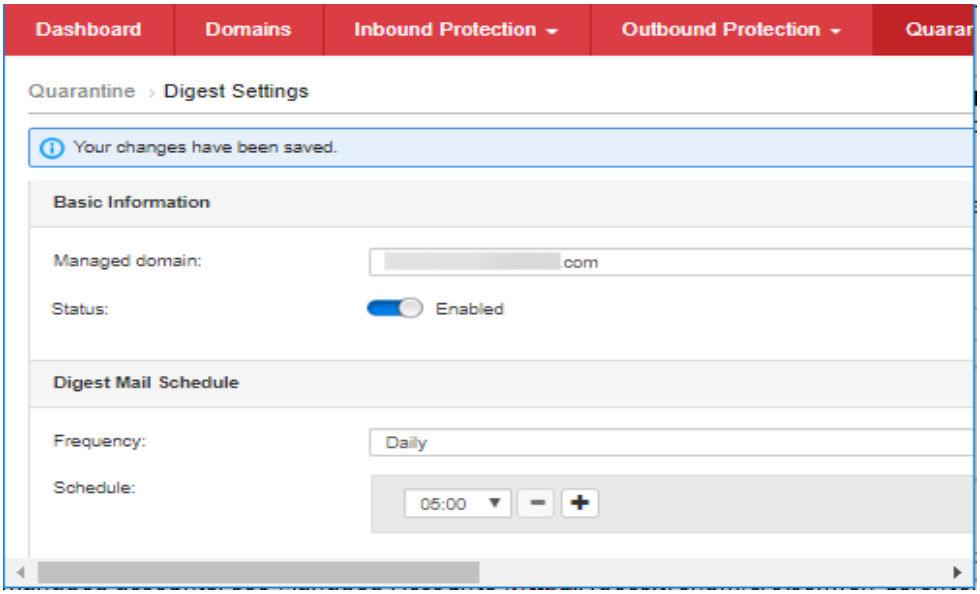


FIGURE 5.2.1: Digest Settings

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 Inline Action is enabled on the Digest Settings screen, recipients can directly manage their quarantined messages from the digest email message. By enabling this function, you can relieve users of the necessity of logging on to the End User Console and manually approving quarantined messages or senders.

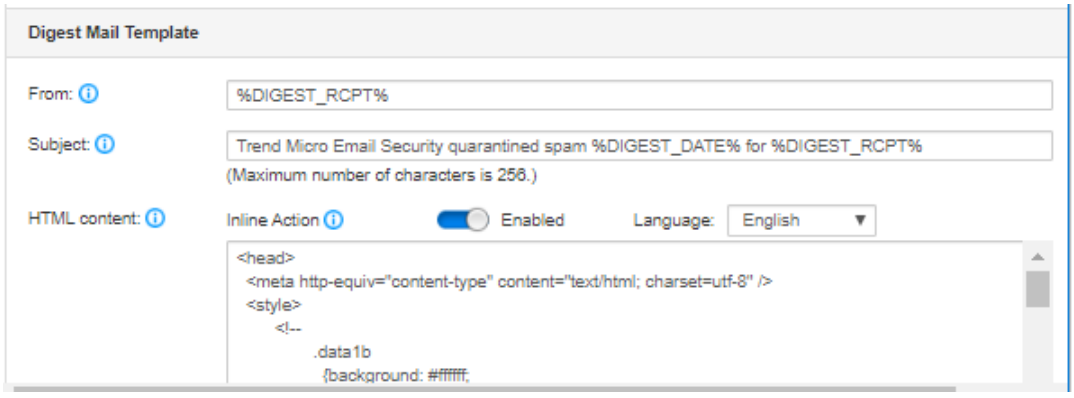
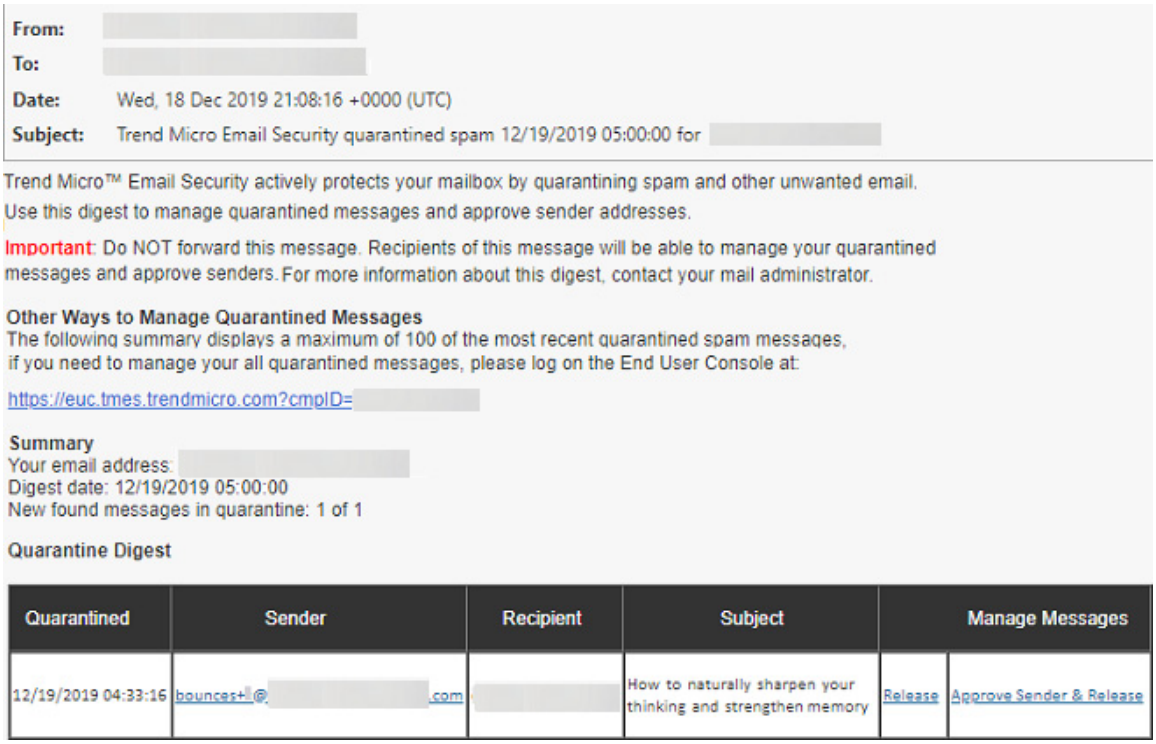


FIGURE 5.2.2: Digest Mail Template

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 Managed Accounts.

For more details, you may refer to Quarantine Digest and EUC Digest settings.



From:
To:
Date: Wed, 18 Dec 2019 21:08:16 +0000 (UTC)
Subject: Trend Micro Email Security quarantined spam 12/19/2019 05:00:00 for

Trend Micro™ Email Security actively protects your mailbox by quarantining spam and other unwanted email.
Use this digest to manage quarantined messages and approve sender addresses.

Important: Do NOT forward this message. Recipients of this message will be able to manage your quarantined messages and approve senders. For more information about this digest, contact your mail administrator.

Other Ways to Manage Quarantined Messages
The following summary displays a maximum of 100 of the most recent quarantined spam messages, if you need to manage your all quarantined messages, please log on the End User Console at:

https://euc.tmes.trendmicro.com?cmpID=

Summary
Your email address:
Digest date: 12/19/2019 05:00:00
New found messages in quarantine: 1 of 1

Quarantine Digest

Quarantined	Sender	Recipient	Subject	Manage Messages	
12/19/2019 04:33:16	bounces+ @ .com		How to naturally sharpen your thinking and strengthen memory	Release	Approve Sender & Release

FIGURE 5.2.3: Example of Digest Quarantine Email

Chapter 6: Querying Logs, Syslog and Report

6.1. Audit Log

The Audit Log screen (**Logs > Audit Log**) enables you to track the administration and user events occurred in Trend Micro Email Security.

Trend Micro Email Security maintains up to 30 days of audit log information.

The Audit Log screen provides the following search criteria:

- **Account and Type**: The account name and the type for which you want to search the audit log.
- **Dates**: The time range for your query.

You can click Search at any time to execute the query again. Use the various criteria fields to restrict your searches.

When you query the audit log, Trend Micro Email Security provides a list of all events that satisfy the criteria.

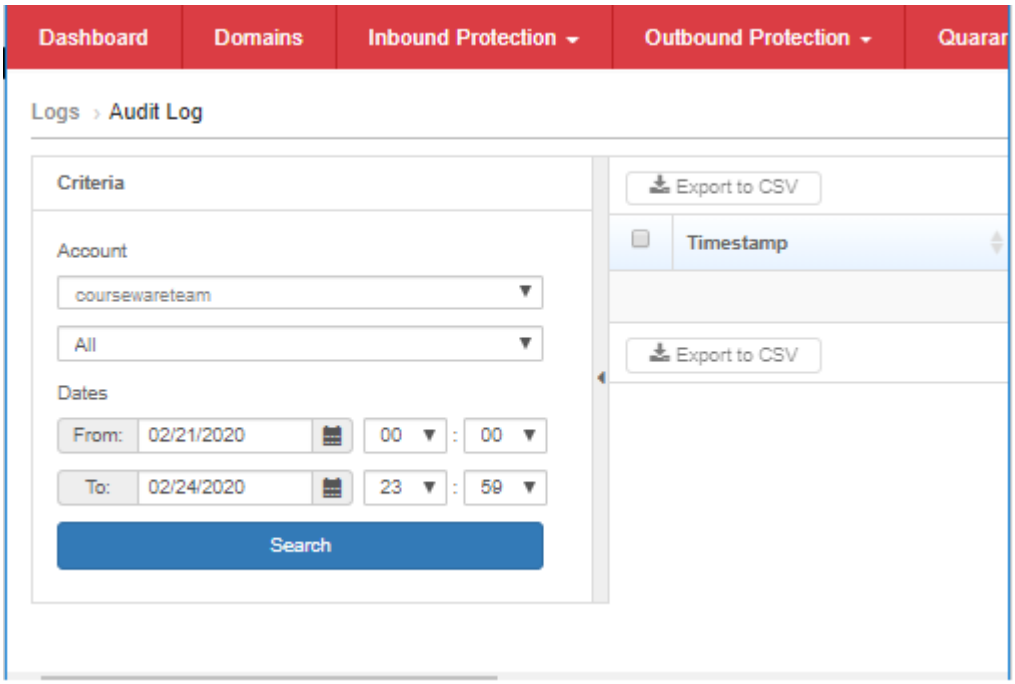


FIGURE 6.1.1: Audit Log Page

To see the detail of an event, click on the **date** under the Dates column.

The Audit Log Details screen displays the following information:

- **User**: The administrator or user name under which the event occurred.
- **Event type**: The type of event that occurred.
- **Dates**: The date and time when the event occurred.
- **Affected domain(s)**: The domains (if any) that were affected by the event.
- **Fields**:
  - **Field**: The name of the fields that were affected by the event.
  - **New Value**: The latest value of the field after the event occurred.
  - **Previous Value**: The previous value of the field (if any) before the event occurred.

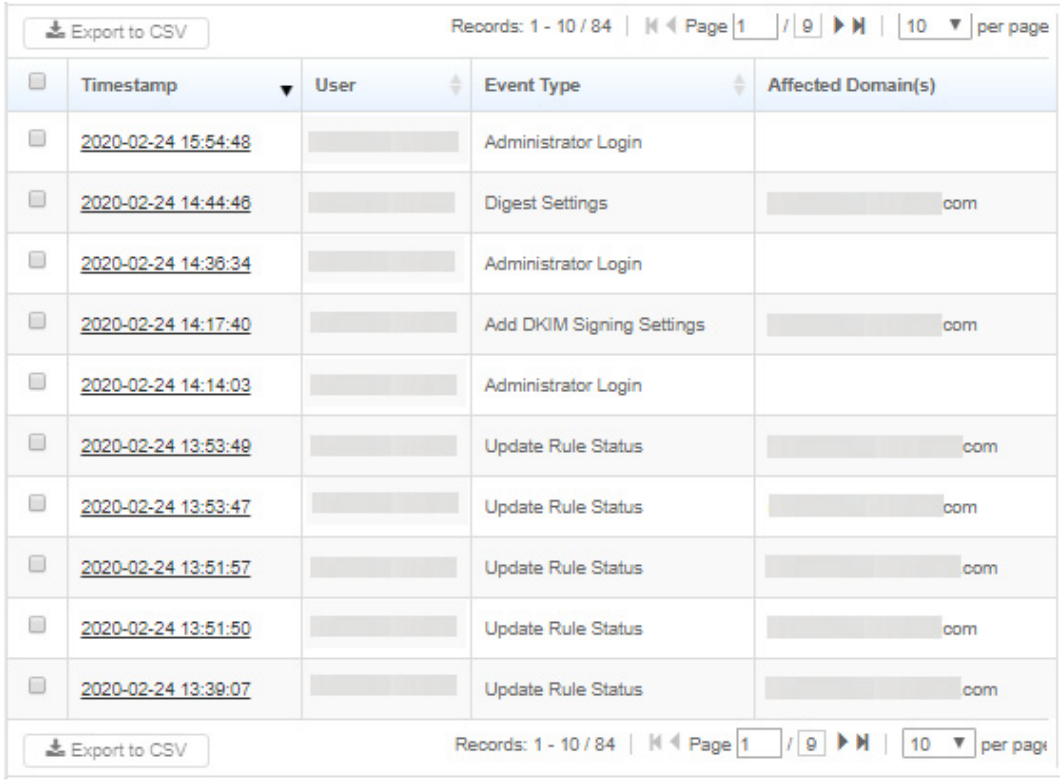


FIGURE 6.1.2: Example of Audit Logs

For more details, refer to Understanding Audit Log.

6.2. Mail Tracking

Mail Tracking Log is designed for you to track email messages that passed through Trend Micro Email Security, including blocked or delivered messages. Trend Micro Email Security maintains up

to 90 days of mail tracking information. Each query can include data for up to 60 continuous days.

NOTE: The sliding window for mail tracking log search is 30 days in Trend Micro Email Security Standard license.

The Mail Tracking page provides the following search criteria:

Search Criterion	Description
Dates	The time range for your query. This is available in the following ranges: • Last 1 hour • Last 24 hours • Last 7 days • Last 14 days • Last 30 days • Custom range
Direction	The direction of the messages: Incoming or Outgoing
Recipient	The recipient email address.
Sender	The sender email address. Pay attention to the following when setting the Recipient and Sender fields: •Specify an exact email address or use wildcards (*) to substitute any characters in a search. In the general format of an email address (local-part@domain), be aware that: – The local part must be a wildcard (*) or a character string that does not start with *. For example, *@example.com or test*@example.com. – The domain must be a wildcard (*) or a character string that does not end with *. For example, example@* or example@*.test.com. – If this field is left blank, *@* is used by default. • Use wildcards (*) strategically to expand or narrow your search results. For example, put a wildcard (*) in the domain part to search by a particular user account on all domains or in the local part to match all accounts on a particular domain.

TABLE 6.1: Mail Tracking Logs Search Criteria Summary

Search Criterion	Description
Type	The type of email traffic that you want to query. • **Accepted traffic**: The messages that were allowed in by Trend Micro Email Security for further processing. – If you select Accepted traffic as your search condition, a summary of email message traffic accepted by Trend Micro Email Security is displayed. For a message that has multiple recipients, the result will be organized as one recipient per entry. • **Blocked traffic**: The attempts to send messages that were stopped by connection-based filtering at the MTA connection level or by Trend Micro Email Security incoming security filtering. – If you select Blocked traffic as your search condition, a summary of sender MTA IP address is displayed, either permanently or temporarily blocked by Trend Micro Email Reputation Services and Trend Micro Email Security incoming security filtering (for incoming messages) or by Trend Micro Email Security relay mail service filtering (for outgoing messages). In the summary, you can find the reason why an email message is blocked.
Action	The last action taken on the message. • **All**: All the actions will be matched for your search. • **Bounced**: Trend Micro Email Security bounced the message back to the sender because the message was rejected by the downstream MTA. • **Temporary delivery error**: Trend Micro Email Security attempted to deliver the message to the downstream MTA but failed due to unexpected errors. This is a transient state of the message, and a message should not remain in this state for an extended period of time. • **Deleted**: Trend Micro Email Security deleted the entire email message according to the matched policy. • **Delivered**: Trend Micro Email Security delivered the message to the downstream MTA. • **Expired**: Trend Micro Email Security bounced the message back to the sender because the message had not been delivered successfully for a long time. • **Quarantined**: Trend Micro Email Security held the message in quarantine awaiting actions because the message triggered certain policy a rule. Quarantined messages can be reviewed and manually deleted or delivered.

TABLE 6.1: Mail Tracking Logs Search Criteria Summary

Search Criterion	Description
	• **Redirected**: Trend Micro Email Security redirected the message to a different recipient according to the matched policy. • **Submitted to sandbox**: Trend Micro Email Security submitted the message to Virtual Analyzer for further analysis. This is a transient state of the message, and the state will change once the Virtual Analyzer analysis result is returned or Virtual Analyzer scan exception is triggered.
Subject	The email message subject. Keyword match is supported, and wildcards (*) are allowed for search.
Message ID	The unique ID of an email message.
Timestamp	The time a message was received.

TABLE 6.1: Mail Tracking Logs Search Criteria Summary

NOTE: Content-based filtering is not included in this category.

Choose the ascending or descending order of time to sort the search results.

When you query the mail tracking information, provide a list of all messages that satisfy the criteria. You can click Search at any time to execute the query again. Use the various criteria fields to restrict your searches.

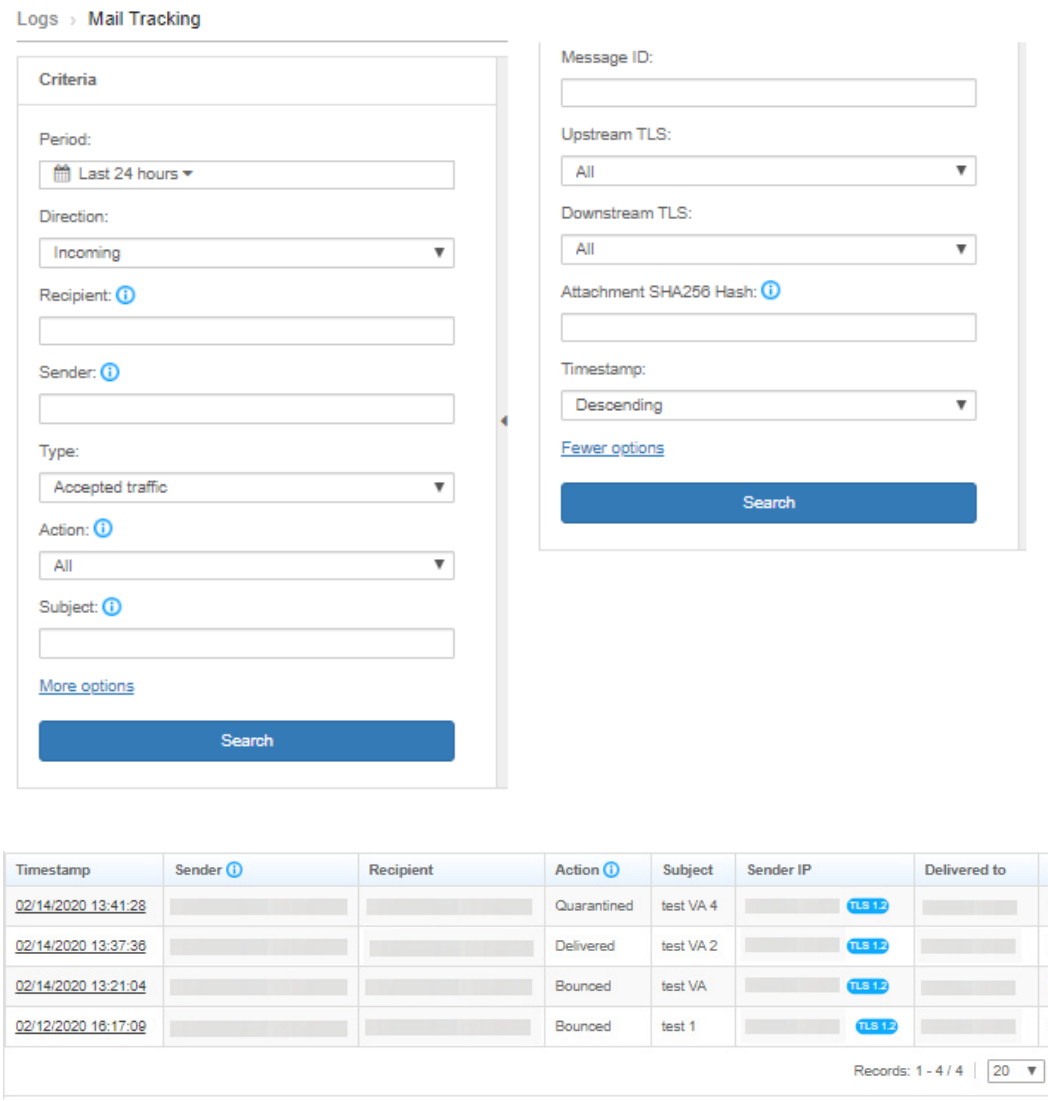
BEST PRACTICE: The most efficient way to track messages is to provide both sender and recipient email addresses within a time range that you want to search. For an email message that has multiple recipients, the result will be organized as one recipient per entry.

If the message you are tracking cannot be located using this strategy, consider the following:

1. Expand the result set by omitting the recipient.
   If the sender is actually blocked by connection-based filtering, the Blocked traffic results that do not match the intended recipient might indicate this. Provide only the sender and time range for a larger result set.

2. Look for other intended recipients of the same message.
   If the sender IP address has a "bad" reputation, mail tracking information will only be kept for the first recipient in a list of recipients. Therefore, the remaining message recipient addresses will not be listed when querying this sender.

3. Expand the result set by omitting the sender.
   If the sender IP address has a "bad" reputation, omit the sender and provide only the recipient. If only the recipient email address is provided, all the messages that pertain to the recipient will be listed.



For more details, refer to Understanding Mail Tracking.

6.3. Policy Events

Policy Events enables you to track the email messages detected with various threats. Trend Micro Email Security maintains up to 30 days of logs for policy events.

Queries include data for up to seven continuous days in one calendar month or across calendar months.

The Policy Events screen provides the following search criteria:

Search Criterion	Description
Dates	The time range for your query.
Direction	The direction of messages.
Recipient	The recipient email address.
Sender	The sender email address.
Subject	The message subject.
Rule Name	The triggered rule that you want to query.
Threat Type	• **Ransomware**: Query the messages that are identified as ransomware. • **Malware**: Query the messages that triggered the malware criteria. When Malware is selected as the threat type, the Detected by field displays with the following options: – **All**: Query all messages. – **Predictive Machine Learning**: Query the messages containing malware, as detected by Predictive Machine Learning. – **Pattern-based scanning**: Query the messages containing malware, as detected by traditional pattern-based scanning. • **Suspicious Objects**: Query the messages that contain suspicious files and URLs. – **All**: Query all messages containing suspicious objects. – **Suspicious Files**: Query all messages containing suspicious files. – **Suspicious URLs**: Query all messages containing suspicious URLs. • **Data Loss Prevention:** Query the messages that triggered the Data Loss Prevention policy. • **Advanced Persistent Threat**: Query the messages that triggered the advanced threat policy. – **Analyzed Advanced Threats (Files)**: Query the messages that are identified as advanced file threats according to Virtual Analyzer and the policy configuration – **Analyzed Advanced Threats (URLs)**: Query the messages that are identified as advanced URL threats according to Virtual Analyzer and the policy configuration – **Probable advanced threats**: Query the messages that are treated as suspicious according to policy configuration or the messages that are not sent to Virtual Analyzer due to exceptions that occurred during analysis. – **All**: Query all messages

TABLE 6.2: Policy Event Logs Search Criteria Description

Search Criterion	Description
Threat Type	• **Business Email Compromise (BEC):** Query the messages that triggered the BEC criteria. – **Detected by Antispam Engine**: Query the messages that are verified to be BEC attacks by the Antispam Engine. – **Detected by writing style analysis**: Query the messages that are verified to be BEC attacks by writing style analysis. – **Suspected by Antispam Engine**: Query the messages that are suspected to be BEC attacks by the Antispam Engine. – **All**: Query all messages. • **Phishing**: Query the messages that triggered the phishing criteria. • **Domain-based Authentication**: Query the messages that failed to pass domain-based authentication. – **All**: Query the messages that failed SPF, DKIM, and DMARC authentication. – **Sender IP Match**: Query the messages that failed Sender IP Match check. – **SPF**: Query the messages that failed SPF check. – **DKIM**: Query the messages that failed DKIM verification. – **DMARC**: Query the messages that failed DMARC authentication. • **Graymail**: Query the messages that triggered the graymail criteria. – Marketing message and newsletter – Social network notification – Forum notification • **Web Reputation**: Query the messages that triggered the Web Reputation criteria. • **Content**: Query the messages that triggered the message content criteria. For example, a message's header, body or attachment matches the specified keywords or expressions. • **Attachment**: Query the messages that triggered the message attachment criteria. • **Scan Exception**: Query the messages that triggered scan exceptions. • **All**: query all messages
Message ID	A unique identifier for the message.

TABLE 6.2: Policy Event Logs Search Criteria Description

When you query the email policy event, Trend Micro Email Security provides a list of all messages that satisfy the criteria.

You can click Search at any time to execute the query again. Use the various criteria fields to restrict your searches.

BEST PRACTICE: The most efficient way to track policy events is to provide both sender and recipient email addresses, message subject and message ID within a time range that you want to search. Recipient and Sender cannot use the wild-card character at the same time.

Detailed policy event information is displayed, including:

- **Timestamp**: The time the policy event occurred. Click on the Timestamp value to view the event details for a given message.
- **Sender**: The sender of the message.
- **Recipient**: The recipient of the message.
- **Message Size**: The size of the message. This information is not always available.
- **Rule Name**: The name of the triggered policy rule that is used to analyze the message.
- **Threat Type**: The threat that triggered the policy event.
- **Risk Rating**: The risk rating of the message identified by Virtual Analyzer.
- **Action**: The action taken on the message. For all the actions, see Actions below:

Action	Description
BCC	Send a blind carbon copy (BCC) to the authorized recipients according to the triggered policy.
Bypass	Ignore and do not intercepted the message.
Change recipient	Change the recipient and redirect the message to a different recipient according to the triggered policy established by the authorized mail administrator of this mail domain.
Clean	Clean the message for viruses.
Delete Attachment	Delete the attachment from the email message.
Deliver	Deliver the message to the downstream MTA responsible for transporting the message to its destination.
Insert X-Header	Add an X-Header to the email message header.
Insert Stamp	Insert a block of text into the email message body.
Send Notification	Delete the message according to the policy established by the authorized mail administrator of this mail domain.
Quarantine	Send a notification message to the recipient when the policy is triggered.
Tag Subject	Insert a block of text defined in the policy into the message subject line.

TABLE 6.3: Policy Events Action Summary

Action	Description
Encryption in progress	Encrypt the message. After encryption is complete, Trend Micro Email Security will queue the message for delivery.
Reject	Block the message before it arrives at Trend Micro Email Security.

TABLE 6.3: Policy Events Action Summary

- **Scanned File Report**: The report for the attached files in the message. If the file is analyzed for advanced threats, the risk level for the file is displayed here. If the report exists, click View Report to see the detailed report.

NOTE: Detailed reports are available only for suspicious files that were analyzed by Virtual Analyzer.

- **Scanned URL Report**: The report for the embedded URLs in the message. If the URL is analyzed as advanced threats, the risk level of the URL is displayed here. If the report exists, click View Report to see the detailed report.

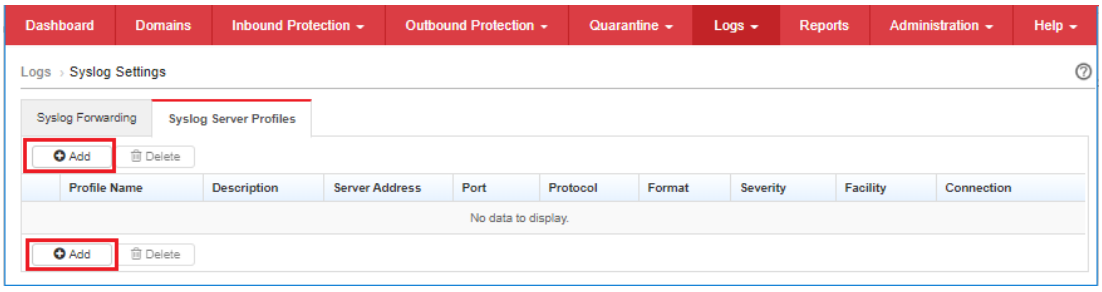
- **DLP Incident**: The information about the DLP incident triggered by the message. Click View Details to check the incident details. This information is available only for messages that violated DLP policies.

TIP: If an email message contains multiple recipients, the result will be organized for each recipient separately.

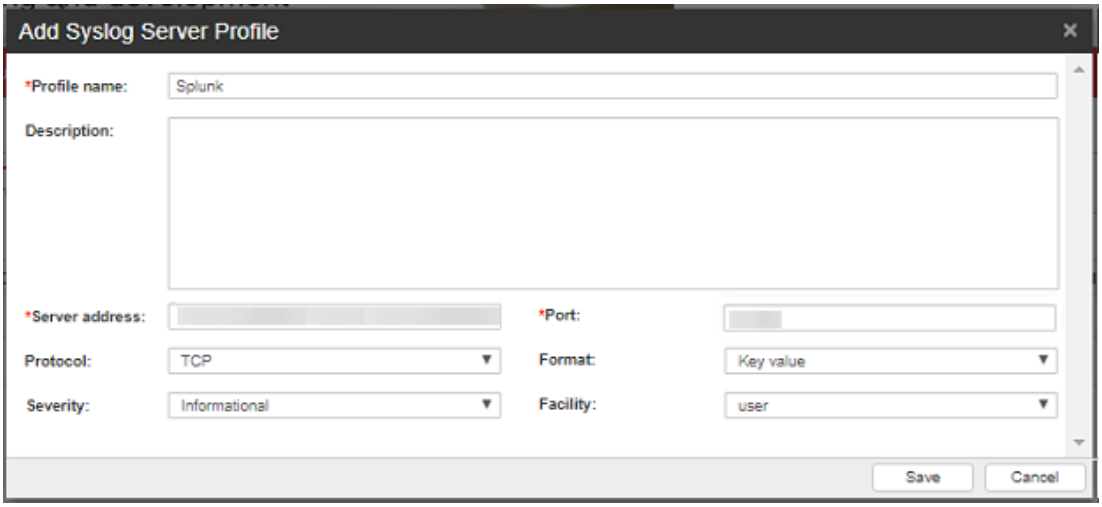
For more details, refer to Understanding Policy Events.

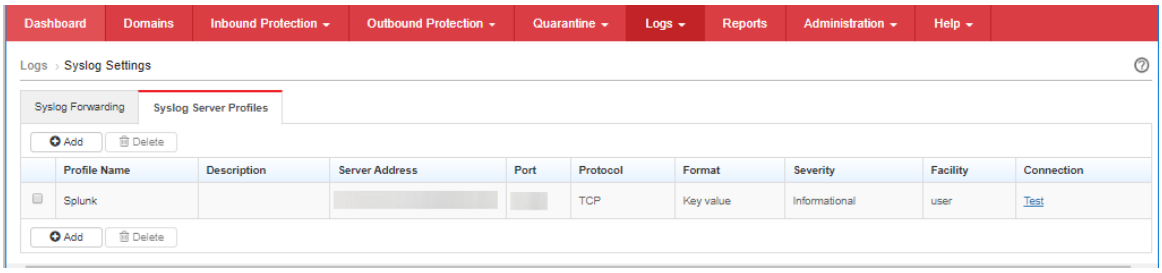
6.4. Syslog

To add a Syslog Server Profile, go to **Logs > Syslog Settings > Syslog Server Profiles tab** then click the **Add** button.



The Add Syslog Server Profile window will pop up, fill out the details then click **Save**.

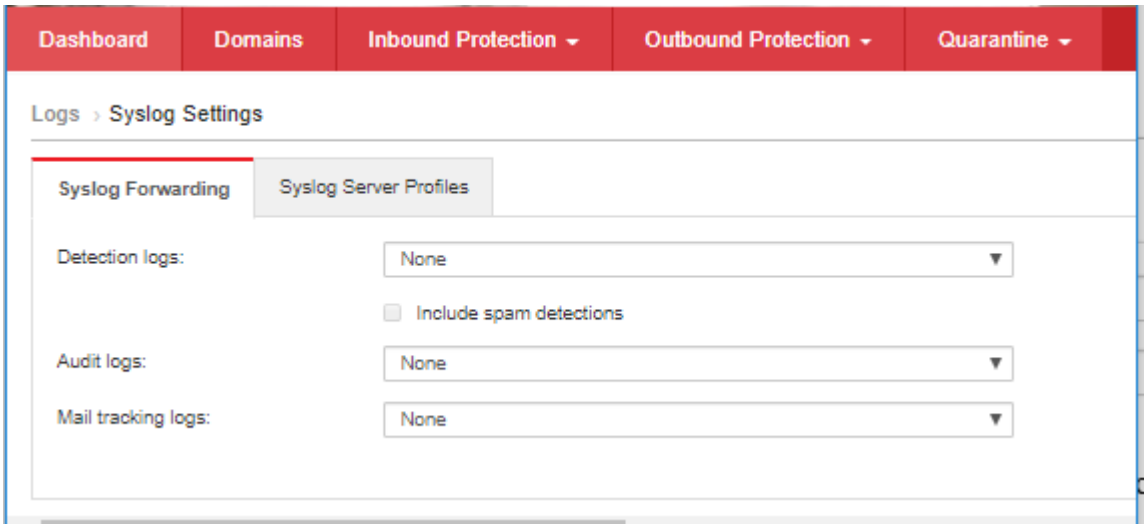




TIP: Click Test for connectivity test.

Configure the syslog server where Trend Micro Email Security forwards different types of logs.

1. Go to **Logs > Syslog Settings**. The Syslog Forwarding tab will be shown by default.



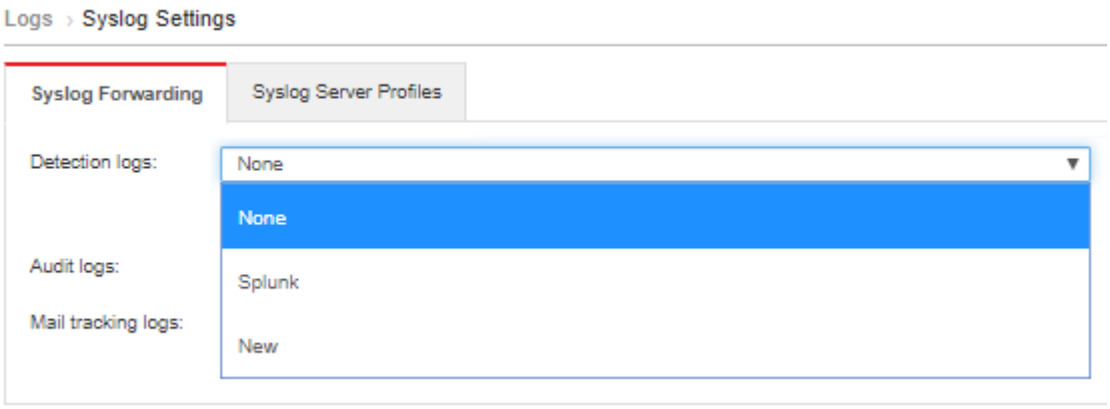
2. From Detection logs drop-down list, select a syslog server for Trend Micro Email Security to forward syslog messages on threat detection events.

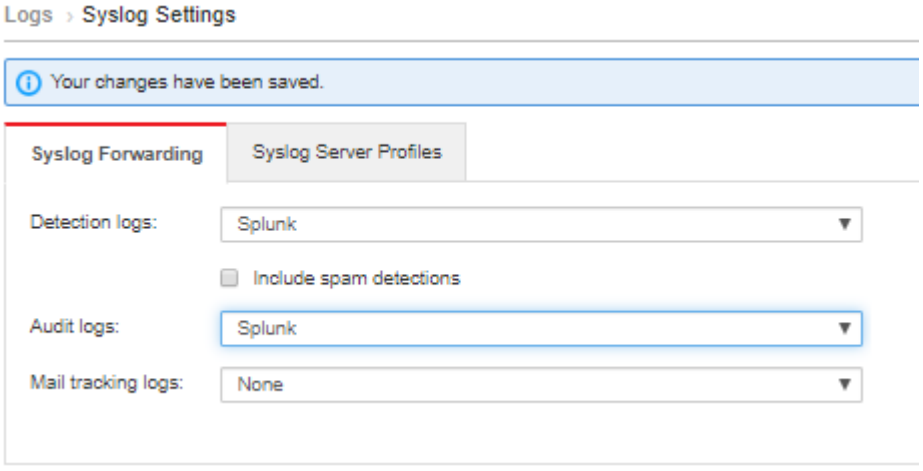
- **None**: Select this option to disable syslog forwarding for this type of logs.
- **New**: Select this option to add a syslog server.

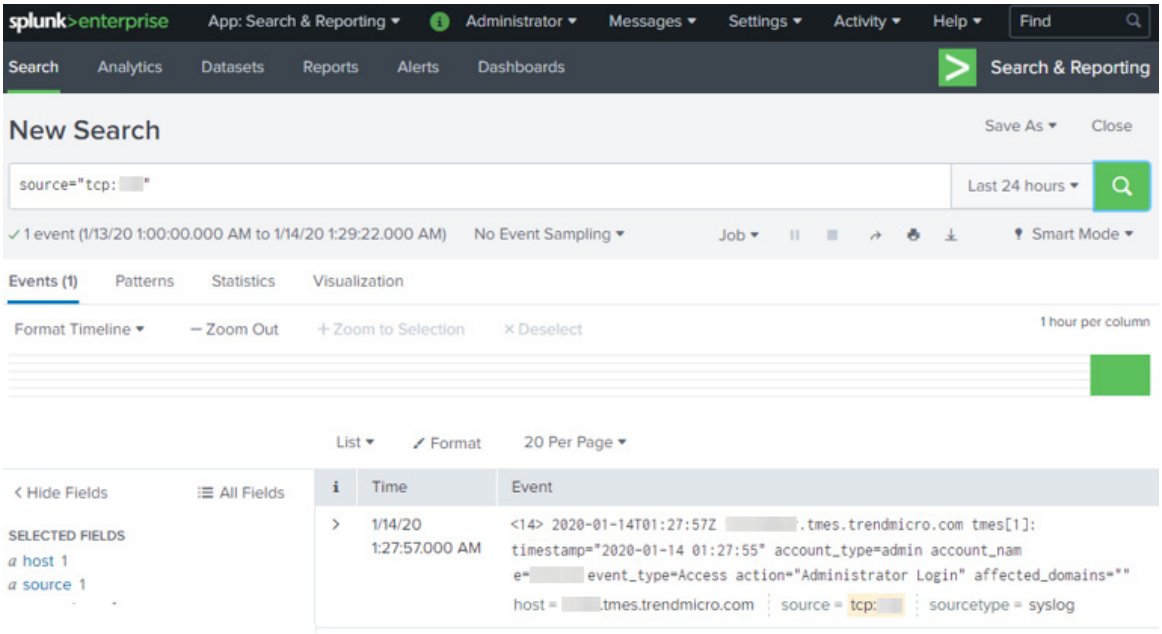
For details on syslog server profiles, see Syslog Server Profiles.

- **Any syslog server profile**: select any profile you configured for forwarding this type of logs.

3. From Audit logs drop-down list, select a syslog server for Trend Micro Email Security to forward syslog messages on audit logs.







For more details, please refer to Syslog Forwarding and Content Mapping Between Log Output and CEF Syslog Type.

6.5. Reports

Trend Micro Email Security provides reports to assist in mitigating threats and optimizing system settings. Generating of reports can be based on a daily, weekly, monthly or quarterly schedule. Trend Micro Email Security offers flexibility in specifying the content for each report.

TIP: The reports are generated in PDF format.

Scheduled reports automatically generate according to the configured schedules. The Schedules tab shows all the report schedules and each schedule contains settings for reports. Reports generate on a specified day of each schedule, which is not configurable.

- Weekly reports generate on every Sunday.
- Monthly reports generate on the first calendar day of every month.
- Quarterly reports generate on the first calendar day of every quarter.

NOTE: This page does not contain any generated reports. To view the generated reports, go to **Reports > My Reports**.

Below are the steps on how to schedule the generation of report:

1. Go to **Reports > Schedules**.

2. Choose the type of scheduled reports you want to generate and click the report type:
   - Daily Report
   - Weekly Report
   - Monthly Report
   - Quarterly Report

3. Complete settings for the scheduled reports.

   - **Status**: Specifies whether to enable the scheduled reports.

   - **Report Content**: Specifies the detailed information contained in the scheduled reports.

   - **Sending schedule**: Specifies how often and when scheduled reports will be sent by email.

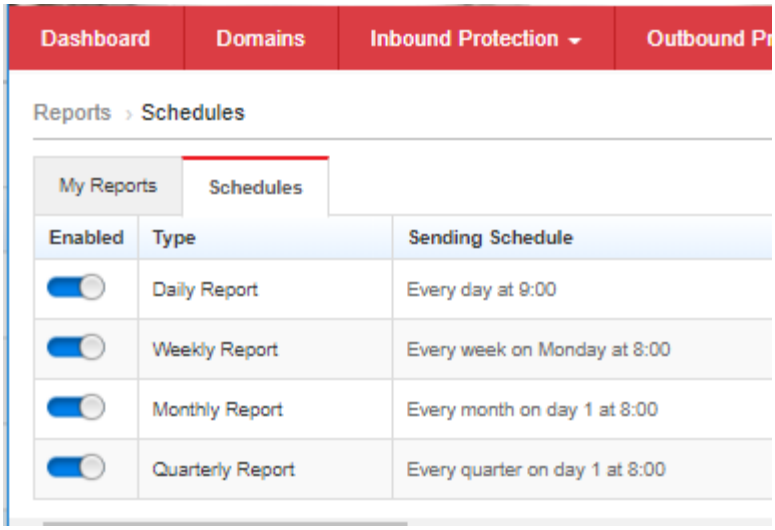
   - **Notify**: Specifies the recipients of the scheduled reports.

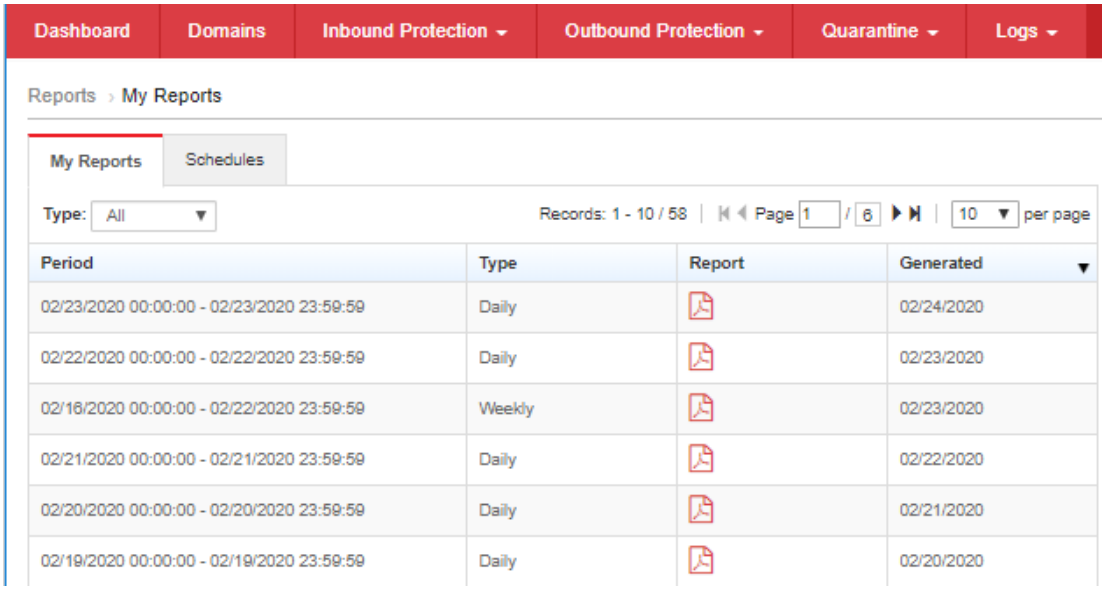
When a monthly report schedule is set to send reports on the 29th, 30th, or 31st day, the report is delivered on the last day of the month for months with fewer days.

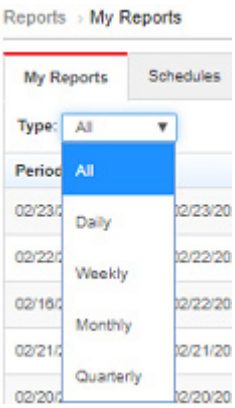
For example, if you select 31, the report is delivered on the 28th (or 29th) in February, and on the 30th in April, June, September, and November. By default, quarterly reports are delivered at 8:00 a.m. on the first day of each calendar quarter, and the default setting is not configurable.

TIP: Make sure the recipients' domains are your managed domains. Separate multiple recipients with a semicolon.

4. Click the **Save** button.







For more details, refer to Reports.

Chapter 7: 2FA and SSO

7.1. Two-Factor Authentication (2FA)

WARNING: If your administrator has enforced two-factor authentication, it means that two-factor authentication must be used every time you log on to the administrator console and it cannot be disabled. Complete the following steps to set up two-factor authentication before you can access the administrator console.

The Trend Micro Email Security administrator console provides two-factor authentication support. Two-factor authentication provides an added layer of security for administrator sub-accounts and prevents unauthorized access to your Trend Micro Email Security administrator console, even if your password is stolen.

After enabling two-factor authentication, administrator sub-accounts and end user accounts need to provide the following authentication credentials each time they sign in:

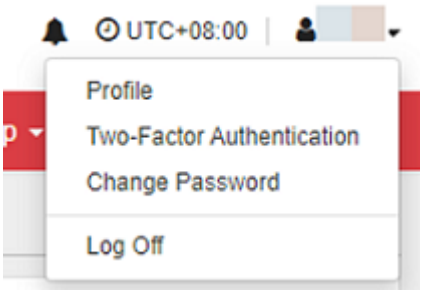
- Local account and password
- A one-time password generated by the Google Authenticator app

NOTE: For end user account, it is assumed that the user is already registered in the End User Console.

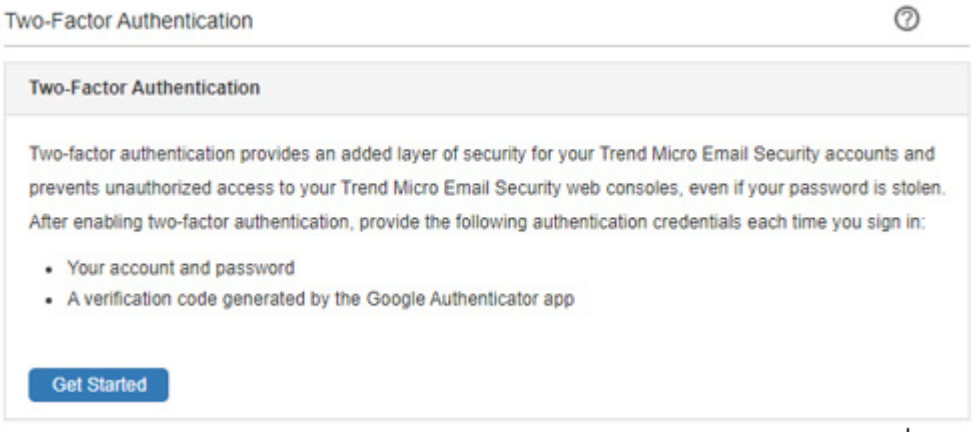
This section describes how to set up two-factor authentication with an administrator sub-account.

1. Login to the Trend Micro Email Security administrator console with your local account and password.

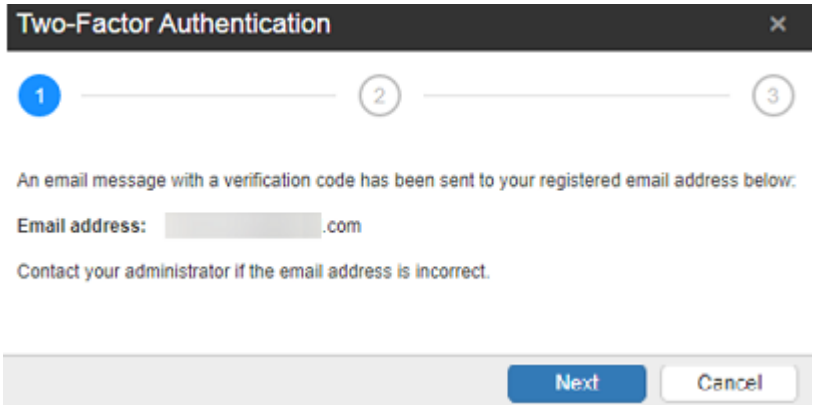
2. Click your **account name** in the top right corner and choose **Two-Factor Authentication** to open the setup wizard.



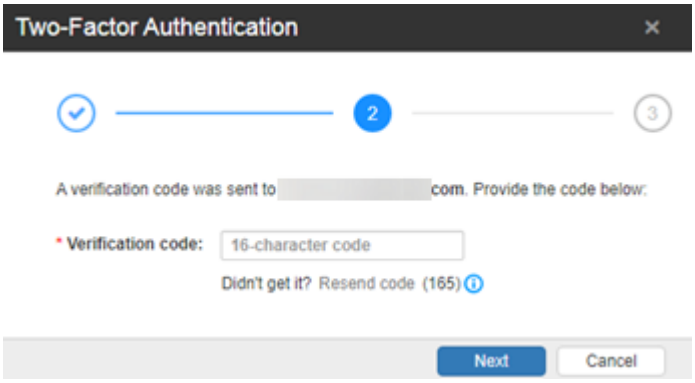
3. Set up two-factor authentication in the wizard.
   a. Click **Get Started**.



   b. Verify your email address then click **Next**.



   c. Obtain the verification code from the email notification sent to your email address. If you did not get the verification code, wait for at least 3 minutes before clicking Resend Code.

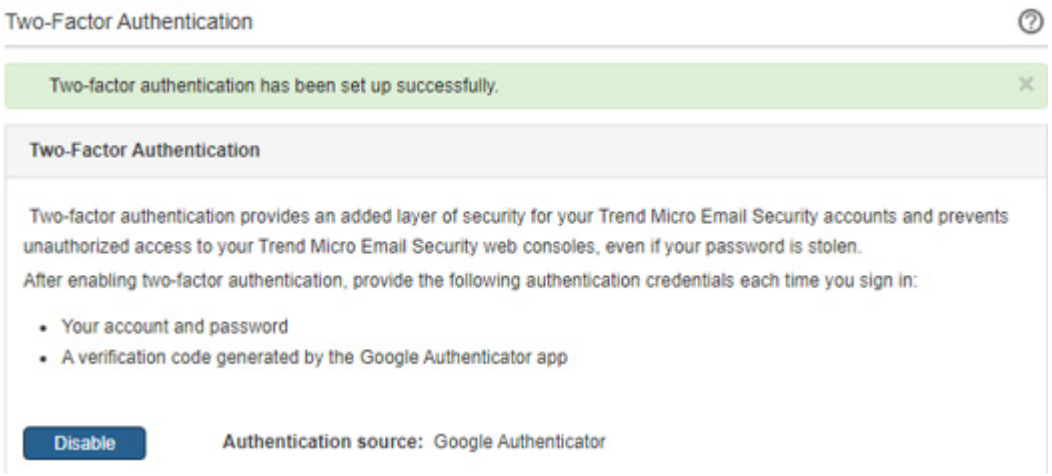


   d. Type the verification code and click **Next**.

   e. Follow the instructions to set up two-factor authentication.

i. Download Google Authenticator either from Apple's App Store or Google Play then install it on your mobile phone.
ii. Add your Trend Micro Email Security account to Google Authenticator by scanning the QR code.
iii. Provide the 6-digit code generated by Google Authenticator to verify that your authentication works properly.

f. Click **Finish**.



Your account will be presented with the two-factor authentication when they try to login.

If you want to disable two-factor authentication, click **Disable** on the Two-Factor Authentication screen. If your administrator has enforced two-factor authentication, click **Reset** to reset two-factor authentication if necessary.

For more details, refer to Setting Up Two-Factor Authentication.

7.2. Single Sign-on (SSO)

Once you enabled single sign-on (SSO) and completed the required settings, sub-accounts and end users can single sign-on to the administrator console with their existing identity provider credentials.

Trend Micro Email Security currently supports the following identity providers for SSO:

- Microsoft Active Directory Federation Services (AD FS) 2.0
- Azure Active Directory (Azure AD)
- Okta

See Logon Methods.

For more details, refer to Configuring Single Sign-On.

Chapter 8: Directory Management

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

Trend Micro Email Security provides a synchronization tool that enables you to synchronize your current groups and email accounts from Open LDAP, Microsoft Active Directory, Microsoft AD Global Catalog, Microsoft Office 365/Azure Active Directory and IBM Domino servers to the Trend Micro Email Security server.

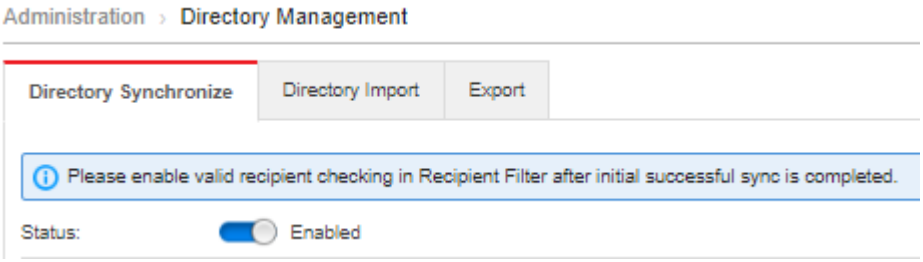
For more details, refer to Directory Management.

The Directory Synchronization Tool automates the importing of directory files for valid recipient email addresses, user groups and email aliases.

The Directory Synchronization Tool provides similar function with the Import User Directory feature on the Directory Import screen.

1. Go to **Administration > Directory Management**.

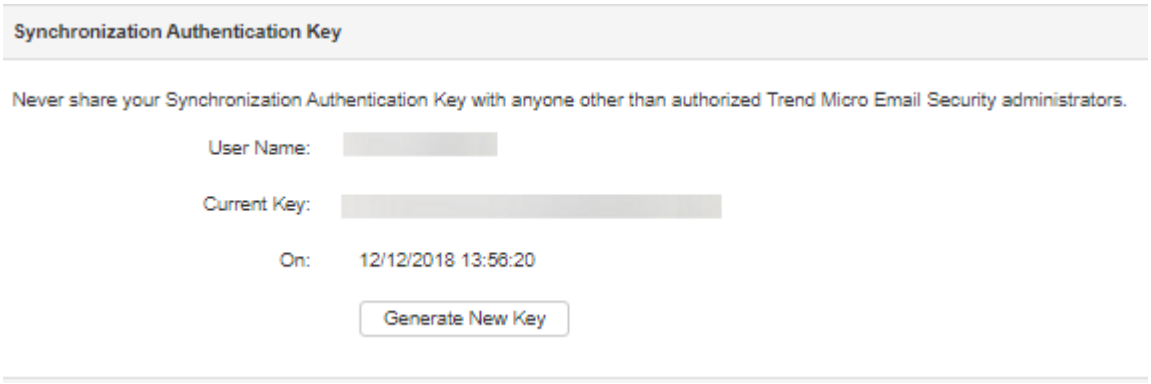
2. On the Directory Synchronize tab, select **Enable**.



3. If Current Key under Synchronization Authentication Key is blank, click **Generate New Key** to generate a key.

The Service Authentication Key is the global unique identifier for your Directory Synchronization Tool to authenticate its access to Trend Micro Email Security.

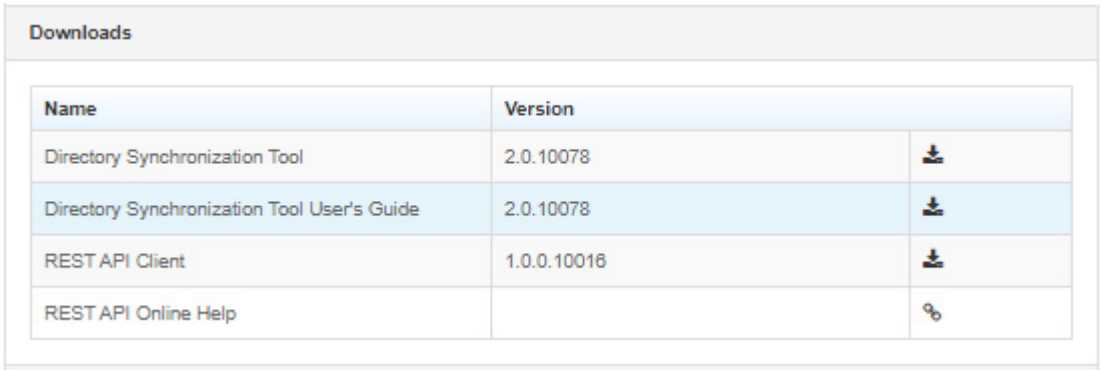
IMPORTANT: Current Key displays the Service Authentication Key that the Directory Synchronization Tool should use. If you generate a new key, you must update the Directory Synchronization Tool to use the new key. The Service Authentication Key allows your Directory Synchronization Tool to communicate with Trend Micro Email Security. Keep the Service Authentication Key private.



4. In the Downloads list, click **download** icon to download the desired items.
   - **Directory Synchronization Tool**: Provided for synchronizing accounts and groups between local directories and the Trend Micro Email Security server.
   - **Directory Synchronization Tool User's Guide**: Available for more information on using the synchronization tool.

5) Save the tool on a local drive.

6) Follow the installation steps to install the tool.



For more details, refer to Installing the Directory Synchronization Tool and Synchronizing User Directories.

For Directory Import method, you can refer to Importing User Directories.

For REST APIs, you can refer to Getting Started with Trend Micro Email Security APIs.

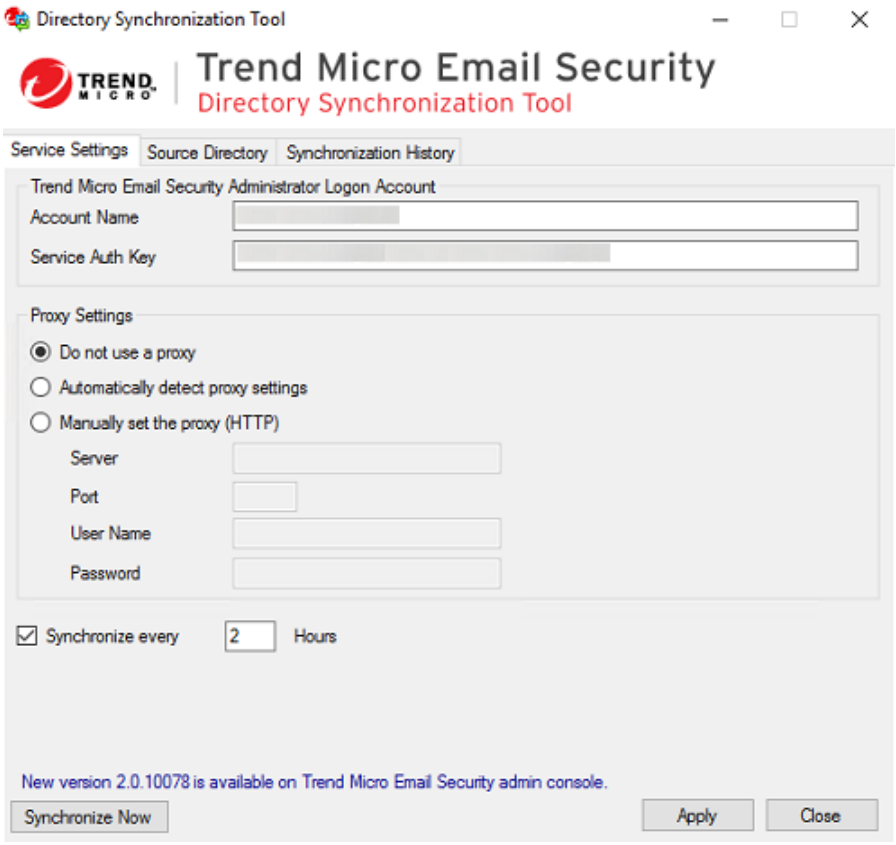


FIGURE 8.1: Directory Synchronization Tool Service Settings

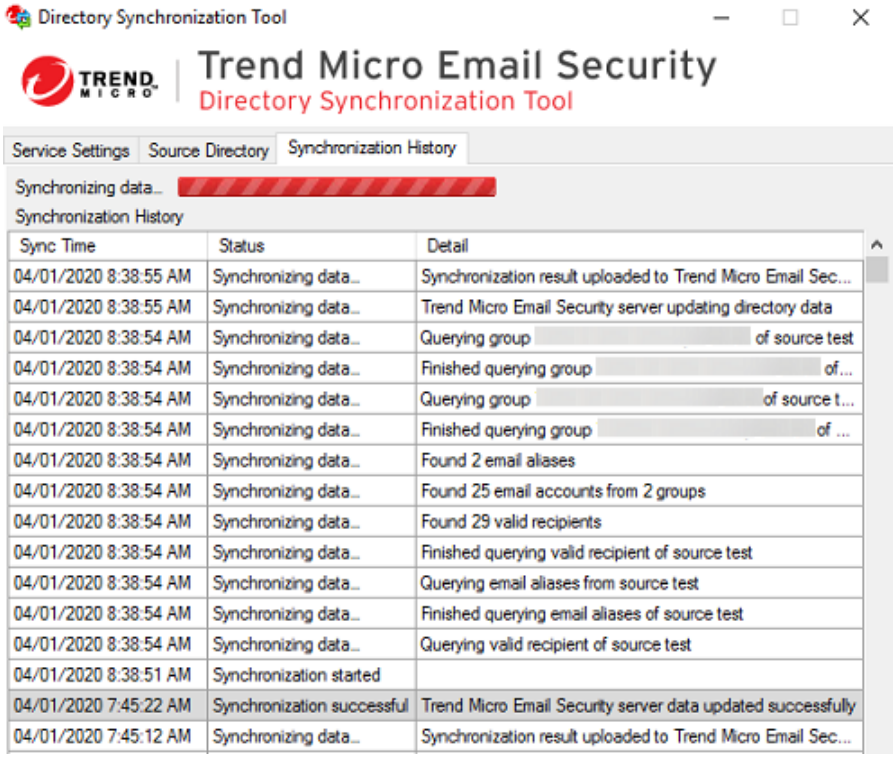


FIGURE 8.2: Directory Synchronization Tool History

Chapter 9: Other Features and Settings

9.1. Dashboard

After logging in to Trend Micro 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 Attacks Detected by Antispam Engine Chart, Top BEC Attacks Detected by Writing Style Analysis Chart, Top Malware Detected by Pattern based Scanning Chart, Top Malware Detected by Predictive Machine Learning Chart, Top Analyzed Advanced Threats (Files) Chart and Top Analyzed Advanced Threats (URLs) Chart can provide the administrator vital information that may indicate if the organization is under attack.

For more details, refer to Top Statistics Tab.

On the other hand, outgoing statistics, like top senders of malware or spam mail, can help identify compromised accounts within the organization.

The dashboard is configurable. Click the **gear** icon on the right side to select which dashboard to show or not to show.

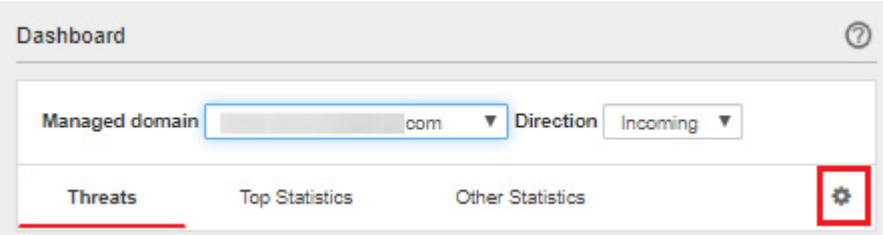


FIGURE 9.1.1: Dashboard Gear Icon

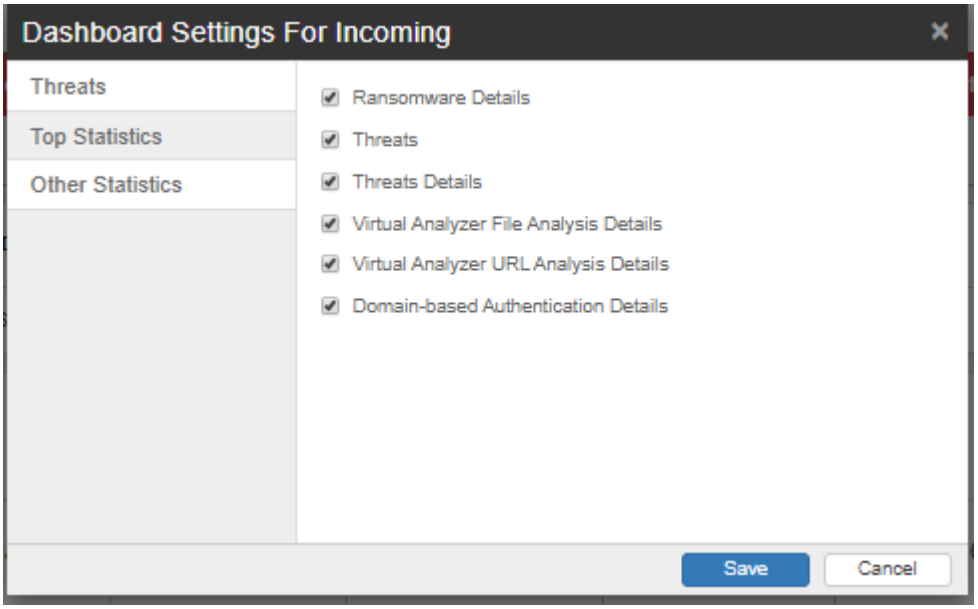


FIGURE 9.1.2: Dashboard Setting Window

The view can be changed, such as: Date, Week, Month, Last 12 Months.

Click one of the following icons to change the view to specific Date, Week, Month, Last 12 Months respectively.

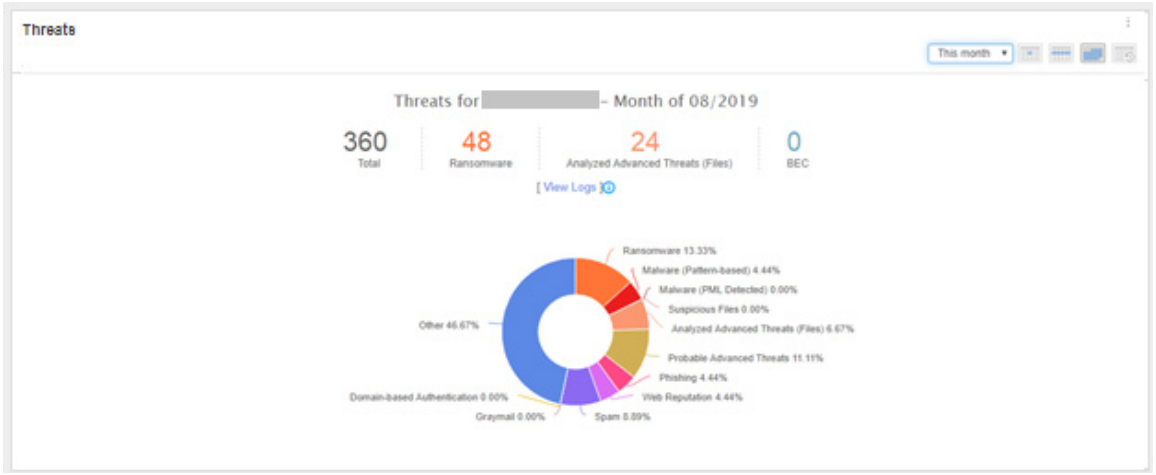


FIGURE 9.1.3: Example of Threats Dashboard

TIP: Regular visit and checking of the dashboard graphs in Trend Micro Email Security is highly recommended.

9.2. Regular Expressions

Regular expressions, often called regex, are sets of symbols and syntactic elements used to match patterns of text. Trend Micro 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.

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

See Keyword Expressions.

9.3. Scan Exceptions

Under certain circumstances, you may want to prevent Trend Micro 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 Trend Micro Email Security is found under **Inbound Protection > Virus Scan > Scan Exceptions** and **Outbound Protection > Virus Scan > Scan Exceptions**.

Inbound Protection › Virus Scan › Scan Exceptions

Exception	Actions
The number of files in a compressed file exceeds 353.	Delete , Notify
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.	Delete , 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

FIGURE 9.3.1: Scan Exception List

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.

9.4. Message Retention and Quarantine Management

The following table shows message retention information:

Item	Retention Period
Quarantined email messages (all regions)	30 days
Message tracking information	90 days
Message queue when customer MTA is unavailable	Up to 10 days

TABLE 9.1: Retention Period Summary

See Feature Limits and Capability Restrictions.

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 **Trend Micro Email Security Administrator console > Quarantine > Query**.

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
   - 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.

NOTE: A recipient or sender can be a specific email address or all addresses from a specific 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 Trend Micro 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.

9.5. General Order of Evaluation

Trend Micro Email Security follows a specific order in evaluating email messages. Knowing this order helps a lot in identifying and troubleshooting email blocking concerns.

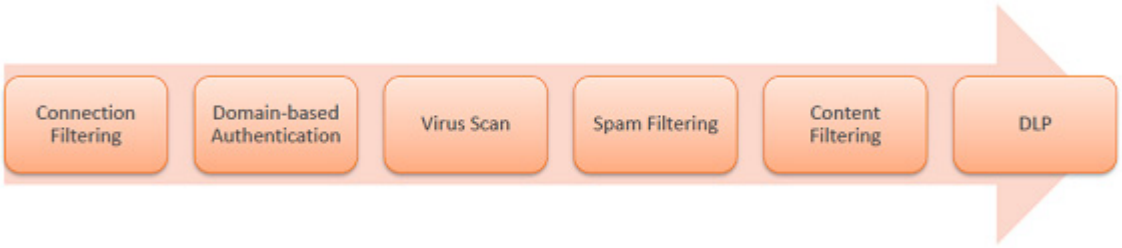


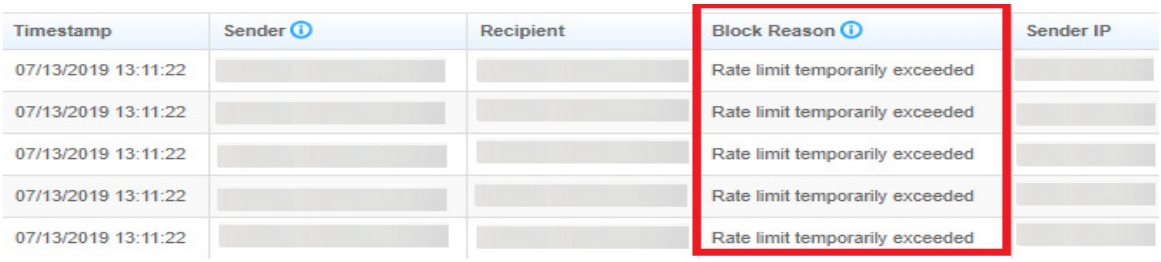
FIGURE 9.6.1: Trend Micro Email Security Order of Evaluation

9.6. Bulk Email Sending

Sending bulk email messages through Trend Email Security is not a supported use case. Trend Micro 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.

Trend Micro 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, Trend Micro Email Security will take actions like temporarily block email messages for a certain period of time.

When this happens, Trend Micro Email Security Mail Tracking will log the rate limited email messages.



Timestamp	Sender	Recipient	Block Reason	Sender IP
07/13/2019 13:11:22			Rate limit temporarily exceeded	
07/13/2019 13:11:22			Rate limit temporarily exceeded	
07/13/2019 13:11:22			Rate limit temporarily exceeded	
07/13/2019 13:11:22			Rate limit temporarily exceeded	
07/13/2019 13:11:22			Rate limit temporarily exceeded	

FIGURE 9.6.1: Example of Rate Limit

This mechanism is Trend Micro 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 Trend Micro Email Security IP address to their blocked list when burst email behavior is detected from one or more of its outbound MTA. Since Trend Micro 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 Trend Micro 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 Trend Micro 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 Trend Micro 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.

9.7. License Renewal

When renewing license for Trend Micro Email Security, make sure that the new Activation Code is properly added to the existing Customer Licensing Portal (CLP) account.

WARNING: Do not create a new account because this will not be associated to your domain registered in Trend Micro Email Security. In the long run, it may lead to improper license mapping and possible service deactivation.

Trend Micro Email Security account is tied to only one Registration and Activation key.

If you have an existing Trend Micro 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 username and password.

3. Under My Products/Services, check Expiration Date and make sure it reflects the correct license expiration date.

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

9.8. Account Management

Trend Micro 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 Trend Micro 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 Trend Micro Email Security administrators.

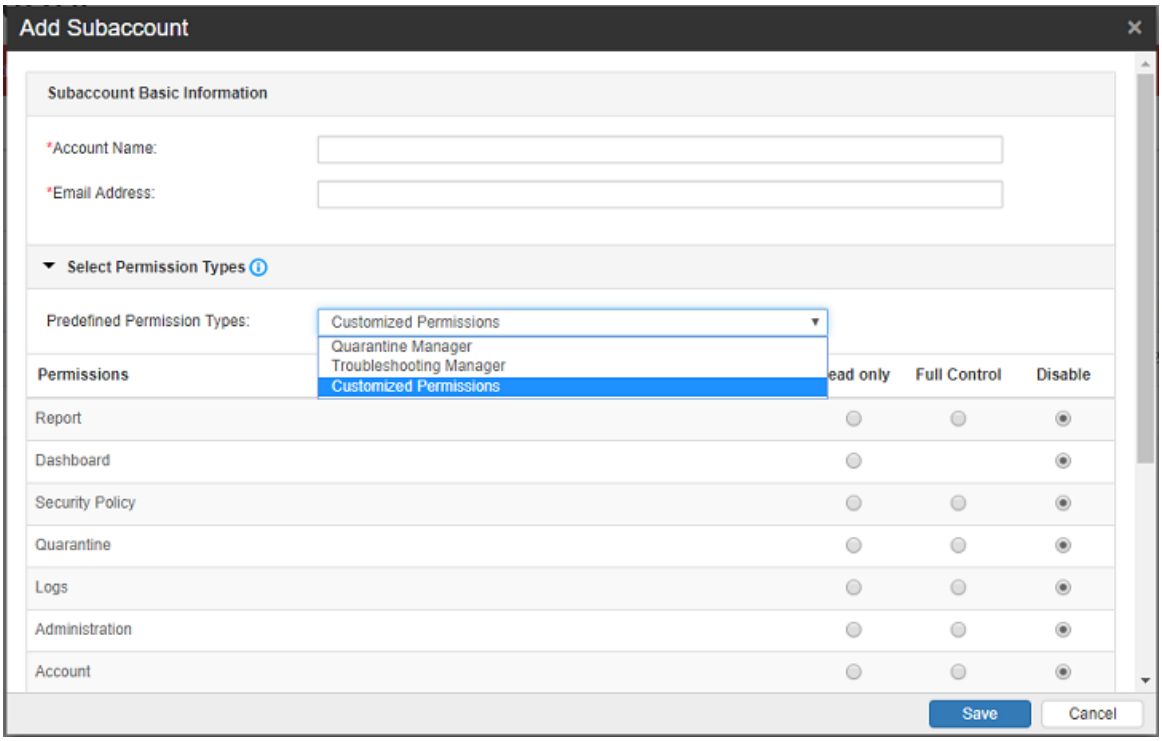
The sub-account can be given permission to one or more of the main account's registered domains. In addition, Role Based Access Control settings are available to provide granular permissions to the sub-account, granting or denying access to certain parts of the administrator console.

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. Trend Micro 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.

9.9. Hand-Off Feature (New)

Hand-Off feature is an enhancement to the previous Deliver Now action (within the policy under Content Filtering, Spam Filtering, and Virus Scan). The previous Deliver Now action will only deliver to the default server. This enhancement will allow customers to specify the deliver destination.

When this action is selected, the matching email will not be scanned by remaining policies. Deliver Now action is still a terminal action which will skip next scan, rules or policies and it will be delivered to the destination specified in the policy.

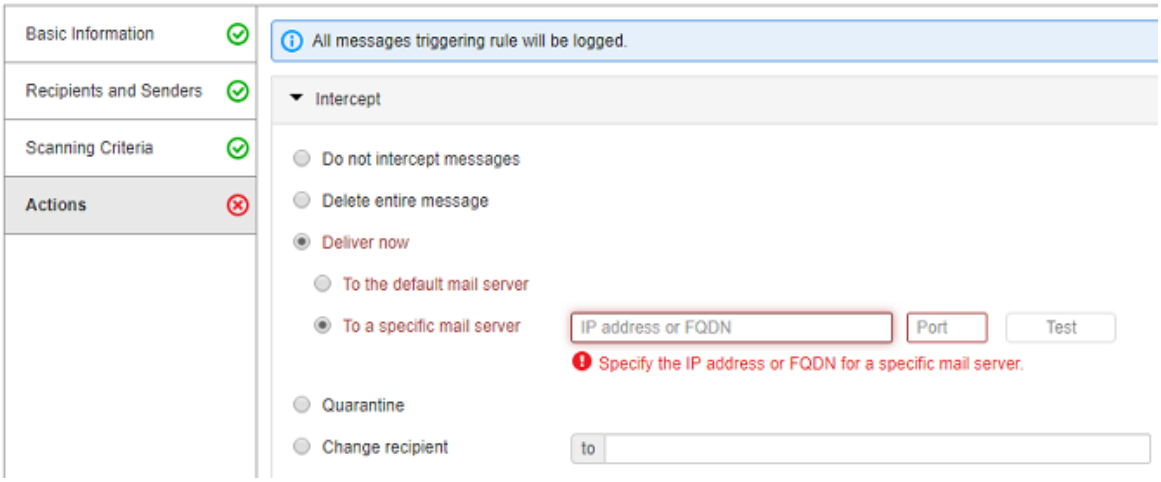


FIGURE 9.9.1: Handoff Feature

9.10. Email Continuity

NOTE: This feature is not included in the Trend Micro Email Security Standard license.

With Email Continuity, Trend Micro Email Security provides a standby email system that gives virtually uninterrupted use of email in the event of a mail server outage.

If a planned or unplanned outage occurs, Trend Micro Email Security will keep your incoming email messages for 10 days. Once your email server is back online within the 10-day period, these messages will be restored to your email server.

A continuity mailbox is available instantly and automatically, providing end users the ability to read, forward, download and reply to any email messages. This enables end users to have continued email access during an outage without requiring any action from IT.

In fact, Trend Micro Email Security will scan the email messages sent from the continuity mailbox based on its default outbound policy.

Administrators can configure and manage Email Continuity records on the Trend Micro Email Security administrator console, and end users will be able to use the continuity mailbox as configured.

For more details, refer to Email Continuity, Adding an Email Continuity Record and Editing an Email Continuity Record.