TrendMicro™
Hosted Email Security

Best Practice Guide
Table of Contents

1  Best Practice Configurations .................................................................................................................. 8
   1.1 Activating a domain ............................................................................................................................. 8
   1.2 Adding Approved/Blocked Sender ....................................................................................................... 8
   1.3 HES order of evaluating emails ......................................................................................................... 8
   1.4 Inbound Emails .................................................................................................................................. 9
      1.4.1 Enable Valid Recipient check ....................................................................................................... 9
      1.4.2 Make sure default virus policy is set to delete ............................................................................. 9
      1.4.3 Add filters to default spam and phish policy ............................................................................... 9
      1.4.4 Avoid long and complex regular expression in Keyword Expression ........................................ 10
   1.5 Outbound Email .................................................................................................................................. 11
      1.5.1 Add additional outbound spam and phish policy ................................................................. 11
   1.6 Securing your Environment ............................................................................................................... 12
      1.6.1 Securing your Mail Server ...................................................................................................... 12
      1.6.2 Securing your Users/Clients .................................................................................................. 12
   1.7 Common Threat preventions ............................................................................................................ 12
      1.7.1 Spoof Emails ............................................................................................................................. 12
      1.7.2 Backscatter (or "outscatter") spam and Directory Harvest Attacks (DHA) Emails ..................... 18
      1.7.3 Zero day unknown Threats ....................................................................................................... 19
      1.7.4 Ransomware/Macro Virus Emails ............................................................................................ 19

2  Product Description ................................................................................................................................. 20
   2.1 Mail Flow ............................................................................................................................................ 21
      2.1.1 Inbound Scanning ....................................................................................................................... 21
         2.1.1.1 IP Reputation-Based Filtering at the MTA Connection Level ............................................. 22
         2.1.1.1.1 Content-Based Filtering at the Message Level .............................................................. 22
         2.1.1.2 General Order of Evaluation ............................................................................................. 23
         2.1.1.3 Sender Filter Order of Evaluation ...................................................................................... 24
         2.1.1.4 IP Reputation Order of Evaluation .................................................................................... 24
         2.1.1.5 Policy Order of Evaluation ............................................................................................... 25
      2.1.2 Outbound Scanning ..................................................................................................................... 26
   2.2 Message Retention .............................................................................................................................. 27

3  Preparation ............................................................................................................................................... 28
   3.1 Service Requirements ....................................................................................................................... 28
   3.2 Default Hosted Email Security Settings ........................................................................................... 28
4 Getting Started .........................................................................................................................29
  4.1 Registration ..........................................................................................................................29
  4.2 Starting the Activation Process .............................................................................................31
    4.2.1 Adding Office 365 Inbound Connectors ........................................................................33
    4.2.2 Adding Office 365 Outbound Connectors .....................................................................34
  4.3 Finalizing Activation .............................................................................................................35
    4.3.1 Repointing MX Records (Best Practice) ........................................................................36
    4.3.2 About MX Records and Hosted Email Security ............................................................38
  4.4 Accessing the Administrator Console ..................................................................................39
    4.4.1 Using CLP to Access the Administrator Console ........................................................39
  5 Management Console ............................................................................................................42
    5.1 Working with the Dashboard ..............................................................................................42
      5.1.1 Summary Chart ............................................................................................................44
      5.1.2 Volume Chart ................................................................................................................45
      5.1.3 Bandwidth Chart .........................................................................................................46
      5.1.4 Threats Chart ...............................................................................................................47
      5.1.5 Threats Details Chart ..................................................................................................49
      5.1.6 Advanced Analysis Details Chart ...............................................................................51
      5.1.7 Top Spam Chart ..........................................................................................................52
      5.1.8 Top Virus Chart ..........................................................................................................53
      5.1.9 Top Analyzed Advanced Threats ..............................................................................54
    5.2 Configuring a Policy ..........................................................................................................56
      5.2.1 Managing Policy Rules ...............................................................................................56
      5.2.2 Selecting User Accounts for Rules ...............................................................................57
      5.2.3 About Rule Target Criteria .........................................................................................57
        5.2.3.1 Configuring Virus or Malicious Code Criteria .......................................................58
          5.2.3.1.1 About Advanced Threat Scan Engine ..........................................................60
        5.2.3.2 Configuring Spam Criteria ..................................................................................60
        5.2.3.3 Configuring Phish Criteria ...................................................................................61
        5.2.3.4 Configuring Marketing Message Criteria ............................................................61
        5.2.3.5 Configuring Social Engineering Attack Criteria .................................................61
        5.2.3.6 Configuring Advanced Criteria .........................................................................63
          5.2.3.6.1 About Keyword Expressions .........................................................................66
            5.2.3.6.1.1 Using Keyword Expressions ...................................................................67
5.2.3.6.2 Using Attachment Name or Extension Criteria .................................................. 68
5.2.3.6.3 Using Attachment MIME Content-type Criteria .................................................. 69
5.2.3.6.4 Using Attachment True File Type Criteria ......................................................... 69
5.2.3.6.5 Using Message Size Criteria ............................................................................ 70
5.2.3.6.6 Using Subject Matches Criteria ....................................................................... 70
5.2.3.6.7 Using Subject is Blank Criteria ....................................................................... 71
5.2.3.6.8 Using Body Matches Criteria .......................................................................... 71
5.2.3.6.9 Using Specified Header Matches Criteria ....................................................... 71
5.2.3.6.10 Using Attachment Content Matches Keyword Criteria .................................. 71
5.2.3.6.11 Using Attachment Size Criteria ..................................................................... 71
5.2.3.6.12 Using Attachment Number Criteria ............................................................... 72
5.2.3.6.13 Using Attachment is Password Protected Criteria .......................................... 72
5.2.3.6.14 Using the Number of Recipients Criteria ....................................................... 73

5.2.4 About Rule Actions ................................................................................................. 73
5.2.4.1 Specifying Rule Actions ...................................................................................... 74
5.2.4.2 "Intercept" Actions ............................................................................................ 74
  5.2.4.2.1 Using the Delete Action ................................................................................. 75
  5.2.4.2.2 Using the Deliver Now Action ...................................................................... 75
  5.2.4.2.3 Using the Change Recipient Action .............................................................. 75
  5.2.4.2.4 Using the Quarantine Action ....................................................................... 76
5.2.4.3 "Modify" Actions ............................................................................................... 76
  5.2.4.3.1 Cleaning Cleanable Viruses ......................................................................... 76
  5.2.4.3.2 Deleting Matching Attachments .................................................................... 76
  5.2.4.3.3 Tagging the Subject Line .............................................................................. 77
  5.2.4.3.4 Inserting a Stamp ....................................................................................... 77
    5.2.4.3.4.4 Configuring Stamps ............................................................................... 78
  5.2.4.3.5 Rule Tokens/Variables .................................................................................. 78
5.2.4.4 "Monitor" Actions .............................................................................................. 79
  5.2.4.4.1 About the Send Notification Action .............................................................. 79
    5.2.4.4.1.5 Configuring Send Notification Actions ..................................................... 80
    5.2.4.4.1.6 Deleting Notifications from Rule Actions ................................................ 80
    5.2.4.4.1.7 Deleting Notifications from Lists of Messages ......................................... 80
5.2.4.4.2 Using the Bcc Action ................................................................. 80
5.2.4.5 "Scan Limitations" Actions ............................................................ 80
  5.2.4.5.1 Rejecting Messages ............................................................... 81
  5.2.4.5.2 Bypassing Messages ............................................................ 81
5.2.4.6 Encrypting Outbound Messages .................................................. 81
5.2.5 Naming and Enabling a Rule .......................................................... 81
5.3 Configuring Sender Filter .................................................................. 82
  5.3.1 Adding Senders ........................................................................... 83
  5.3.2 Editing Senders ........................................................................... 84
5.4 Understanding IP Reputation ............................................................. 85
  5.4.1 About Dynamic IP Reputation Settings .......................................... 85
  5.4.2 About Standard IP Reputation Settings .......................................... 86
  5.4.3 About Approved and Blocked IP Addresses ..................................... 87
  5.4.4 Troubleshooting Issues ................................................................. 88
5.5 Understanding Advanced Protection .................................................. 88
  5.5.1 About Transport Layer Security (TLS) ............................................ 88
    5.5.1.1 Testing TLS ........................................................................... 89
    5.5.1.2 Adding TLS Peers ................................................................. 90
    5.5.1.3 Editing TLS Peers ............................................................... 91
  5.5.2 About Sender Policy Framework (SPF) ........................................... 91
    5.5.2.1 Enabling or Disabling Sender Policy Framework (SPF) .............. 92
    5.5.2.2 Adding an SPF Peer to the Ignored List ................................... 93
    5.5.2.3 Editing an SPF Peer in the Ignored List ................................... 93
    5.5.2.4 Deleting SPF Peers from Ignored List ..................................... 93
5.6 Understanding Quarantine ................................................................. 94
  5.6.1 Querying the Quarantine .............................................................. 94
  5.6.2 About the Quarantine Digest ......................................................... 96
    5.6.2.1 Configuring the Quarantine Digest ......................................... 97
5.7 Understanding Mail Tracking ............................................................ 99
  5.7.1 About the Blocked Traffic Tab ...................................................... 100
  5.7.2 About the Accepted Traffic Tab .................................................... 101
  5.7.3 About the Unresolved Traffic Tab ................................................ 102
  5.7.4 Social Engineering Attack Log Details ......................................... 103
5.8 Understanding Policy Events ............................................................ 105
1 Best Practice Configurations

1.1 Activating a domain

When activating a domain in Hosted Email Security, Trend Micro recommends making these changes to your MX record to reduce the chance of security vulnerability or an interruption of service while repointing your MX record.

See Repointing MX Records (Best Practice)

1.2 Adding Approved/Blocked Sender

- Approved Senders

  Email messages from senders added to this list are not subject to IP reputation-based, spam, phish, or marketing message filtering. Hosted Email Security still performs malware and attachment scanning on all messages received and takes the action configured in policy rules after detecting a malware threat or an attachment policy violation.

  Go to Sender Filter > Approved Senders to display this screen.

- Blocked Senders

  Hosted Email Security automatically blocks messages sent from addresses or domains added to the blocked list without subjecting the messages to any scanning.

  Go to Sender Filter > Blocked Senders to display this screen.

See Configuring Sender Filter

1.3 HES order of evaluating emails

Hosted Email Security follow a certain order on how it evaluate each email that pass through it servers.

See General Order of Evaluation
### 1.4 Inbound Emails

#### 1.4.1 Enable Valid Recipient check

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

See [Using Directory Management](#)

#### 1.4.2 Make sure default virus policy is set to delete

By default the virus policy is already set to delete but if it was modified to other action set it back to delete to avoid any virus entering your system.

1. Log in to HES management console.
2. Go to Policy and look for Virus policy

   ![Policy screenshot]

3. Make sure action is set to delete.

#### 1.4.3 Add filters to default spam and phish policy

Increase spam detection level and enable Social Engineer attack including advance analysis to identify threats.

1. Log in to HES management console.
2. Go to Policy and look for Spam and policy

   ![Policy screenshot]
3. Click “And message attribute match”

4. Check all boxes and set Spam check to a higher level. Note that setting spam check higher might lead to more false positive but it can also reduce false negative emails and avoid malicious emails in.

1.4.4 Avoid long and complex regular expression in Keyword Expression

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

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

See About Keyword Expressions
1.5 **Outbound Email**

1.5.1 **Add additional outbound spam and phish policy**

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

To control your outbound spam and phish emails it’s recommended to create new outbound spam and phish policy.

1. Log in to HES management console.
2. Go to Policy and click Add.
3. Change policy to “outgoing message”
4. Click Sender and add your domain the save. Click Next.
5. Select “Message detected as” and tick all boxes. Click Next once done.
6. Select your action and click Next.
7. Input policy name and click Save.
1.6 Securing your Environment
Trend Micro Hosted Email Security prevents spam from entering your mail servers. However, there might be instances when you will still receive spam even after subscribing to HES. This occurs when the mail server is set to accept mails from another host. As a result, spam goes directly to the mail server without passing through the HES / HES - Inbound Filtering servers. To avoid this, here are the best practices in preventing spam.

1.6.1 Securing your Mail Server

1. Lock down your firewall

Make sure that all unnecessary ports and IP addresses are closed and blocked. Only allow IP addresses from trusted ones such as the ones from HES.

You may find HES server IP addresses below:
HES IP addresses

2. Install On-premise mail server Anti-Malware

Although most of the malware and spam are blocked by HES, there are a few instances when a malware/spam gets through to your mail server. This may be caused by having unnecessary ports and IP addresses open on your network, or it may not have been detected by the anti-spam/anti-malware patterns of HES at that time. So it will be best to have an On-premise scanner to combat this.

3. Only use one MX record for your domain

This MX record should be pointing to HES. It’s to make sure that all inbound mails will be forced to go through HES for filtering before it goes to your mail server.

See Repointing MX Records (Best Practice)

4. Disable all open mail relay on your network.

1.6.2 Securing your Users/Clients

1. Do NOT click unknown links

Any links in email or on the internet should not be clicked unless it’s from a trusted site.

2. Do NOT subscribe to untrusted newsletters

Unless it’s absolutely necessary and you’re sure that the site can be trusted.

1.7 Common Threat preventions

1.7.1 Spoof Emails

Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).
Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from a legitimate source when it actually was sent from a malicious one.

To stop receiving emails from spoofed senders, aside from Securing your Mail Server and Securing your Users/Clients follow instructions below:

1. Avoid putting managed email address and domain in the Sender Filter Approved Sender or EUQ Approved Sender as it will bypass IP reputation checking and Spam/Phish Rule scanning.
   
   Check if the spoofed sender is listed on the Approved Senders List on the HES / HES - Inbound Filtering console.
   
   If the spoofed sender is listed, remove the spoofed sender from the Approved Senders List.

   If not, check if the end-user is registered to the HES/HES - Inbound Filtering Web EUQ. If the owner of the spoofed address is registered to HES Web EUQ, make sure that the address is also not listed in the Web-EUQ Approved Senders list. To do this, you can:
   
   • Ask the owner of the spoofed email address.
   
   • On the HES / HES - Inbound Filtering console, go to Administration > End-User password and then query the email address.

2. Make sure that Incoming Spam/Phish Rule is enabled and properly configure.
   See Configuring Spam Criteria

3. Increase the aggressiveness of the Dynamic IP Reputation Settings.
   
   See Understanding IP Reputation.

4. Create a policy for filtering spoofed emails from same domain as recipient.
**Warning:**

Make sure inter-domain emails are not routed to the internet.

---

1. On your browser, log in to HES management console
2. Go to Policy > Click Add
3. On This rule will apply to > Select Incoming message
4. Click Recipients > Select addresses > My Domains > Select your domain
5. Click Add > Click Save
6. Click Sender > Select addresses > My Domains > Select your domain
7. Click Add > Click Save
8. Click Next
9. Select Advanced > Select Any Match
10. Select Specified header matches > Click keyword expressions
11. Click Save
12. Click Save
5. Enable SPF checking.

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

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

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

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

- Create SPF txt record for your domain

- Enable SPF checking in HES

- Create a policy to track emails tagged by HES SPF checking.
  1. On your browser, log in to HES management console
  2. Go to Policy > Click Add
  3. On This rule will apply to > Select Incoming message
  4. Click Recipients > Select addresses > My Domains > Select your domain
  5. Click Add > Click Save
6. Click Next

7. On criteria select Advance then check Specified header matches.

<table>
<thead>
<tr>
<th>No criteria</th>
<th>Message contains</th>
<th>antispy or malicious code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message detected as</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td>All Match</td>
<td>Any Match</td>
</tr>
<tr>
<td>Attachment is</td>
<td>name or extension</td>
<td></td>
</tr>
<tr>
<td>Attachment is</td>
<td>IMAGE content type</td>
<td></td>
</tr>
<tr>
<td>Attachment is</td>
<td>text file type</td>
<td></td>
</tr>
<tr>
<td>Message size is</td>
<td>&gt; 10 MB</td>
<td></td>
</tr>
<tr>
<td>Subject matches</td>
<td>keyword expressions</td>
<td></td>
</tr>
<tr>
<td>Subject is</td>
<td>blank</td>
<td></td>
</tr>
<tr>
<td>Body matches</td>
<td>keyword expressions</td>
<td></td>
</tr>
<tr>
<td>Specified header matches</td>
<td>keyword expressions</td>
<td></td>
</tr>
<tr>
<td>Attachment content matches</td>
<td>keyword expressions</td>
<td></td>
</tr>
<tr>
<td>Attachment content size is</td>
<td>&gt; 5 MB</td>
<td></td>
</tr>
<tr>
<td>Attachment number is</td>
<td>&gt; 20</td>
<td></td>
</tr>
<tr>
<td>Attachment is</td>
<td>password protected</td>
<td></td>
</tr>
<tr>
<td>Recipient number is</td>
<td>&gt; 50</td>
<td></td>
</tr>
</tbody>
</table>

8. Click Keyword expressions beside header match.

9. Check all the boxes and click Add.
10. Type List name “ex. SPF match” and under Match select Any specified. Click Add.

11. Add keyword “X-TM-Received-SPF: SPF result” then save.  
Ex. X-TM-Received-SPF: Fail  
See [Enabling or Disabling Sender Policy Framework (SPF)](...) for SPF results.

12. Click Save.
13. Select created Keyword and click add then save.

14. Click Next.

15. Select chosen Actions and click next.

16. Type a Rule Name and save.

1.7.2 Backscatter (or "outscatter") spam and Directory Harvest Attacks (DHA) Emails

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

- Enable Directory management to prevent these types of malicious emails.
  See About Directory Management
1.7.3 Zero day unknown Threats

- Enable Advance Threat Scan Engine and Perform advanced analysis to identify high risk objects.

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

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

To integrate HES with Deep Discovery Analyzer as a Service (DDAas):

1. Log in to HES management console.
2. Go to Policy and select Viruses or Malicious Code.
3. Under Specify advanced settings, tick the Enable Advance Threat Scan Engine and Perform advanced analysis to identify high risk objects options.
4. Click Save.

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

1.7.4 Ransomware/Macro Virus Emails

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.

Increase protection from Ransomware threats in HES by following guide below.

See Ransomware protection using Hosted Email Security
2 Product Description

Trend Micro™ Hosted Email Security is a no-maintenance solution that delivers continuously updated protection to stop spam, phishing, and malware before they reach your network.

Using Trend Micro Hosted Email Security, mail administrators can set up rules to remove detected viruses and other malware from incoming messages before they reach the corporate network. Administrators can quarantine detected spam and other inappropriate messages. Then, intended message recipients or mail administrators can choose to release or delete the quarantined messages.
2.1 Mail Flow

2.1.1 Inbound Scanning

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

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

2. The originating MTA routes messages to Hosted Email Security.

3. The Hosted Email Security MTA accepts the connection from the originating mail server.

4. Hosted Email Security performs IP reputation-based filtering at the MTA connection level to decide on an action to take. Actions include the following:

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

   See [IP Reputation-Based Filtering at the MTA Connection Level](#).

5. Hosted Email Security examines the message contents to determine whether the message contains malware such as a virus, or if it is spam, and so on.

   See [Content-Based Filtering at the Message Level](#).

6. Assuming that a message is slated for delivery according to the domain policy rules, the Hosted Email Security MTA routes the message to the original example.com Inbound Server.
2.1.1.1 IP Reputation-Based Filtering at the MTA Connection Level

When an originating or upstream MTA attempts to connect to a Hosted Email Security MTA, the Hosted Email Security MTA queries Trend Micro Email Reputation Services (ERS) to determine whether the IP address of the upstream MTA has a "trustworthy" reputation in the database.

Based on the upstream MTA's reputation and the selections on the Hosted Email Security IP Reputation Settings screen, Hosted Email Security may terminate the connection, rejecting the messages. This is IP reputation-based filtering at the MTA connection level.

Hosted Email Security terminates upstream MTA connections in the following ways:

- If the sending IP address is a known source of spam, the IP address of the sending server is marked "untrustworthy" according to the reputation database. Hosted Email Security permanently rejects connection attempts from such IP addresses by responding with a 550 error (a rejection of the requested connection).

- If the sender's computer is part of a botnet or is a zombie PC, the IP address can be found in the Email Reputation Services (ERS) dynamic reputation database that identifies spam sources as they emerge and for as long as they are active. Hosted Email Security informs the sending server that Hosted Email Security is temporarily unavailable by responding with a 450 error (a temporary failure of the requested connection). If the sending server is legitimate, it will try again later.

Hosted Email Security performs this filtering prior to receiving the actual message; therefore the content of the message is not yet scanned.

To manually override IP reputation-based filtering at the MTA connection level, add IP addresses to the lists on the Approved and Blocked IP Addresses screen.

2.1.1.1.1 Content-Based Filtering at the Message Level

When an originating or upstream MTA attempts to connect to a Hosted Email Security MTA, the Hosted Email Security MTA queries Trend Micro Email Reputation Services (ERS) to determine whether the IP address of the upstream MTA has a "trustworthy" reputation in the database.

Based on the upstream MTA's reputation and the selections on the Hosted Email Security IP Reputation Settings screen, Hosted Email Security may terminate the connection, rejecting the messages. This is IP reputation-based filtering at the MTA connection level.

Hosted Email Security terminates upstream MTA connections in the following ways:

- If the sending IP address is a known source of spam, the IP address of the sending server is marked "untrustworthy" according to the reputation database. Hosted Email Security permanently rejects connection attempts from such IP addresses by responding with a 550 error (a rejection of the requested connection).

- If the sender's computer is part of a botnet or is a zombie PC, the IP address can be found in the Email Reputation Services (ERS) dynamic reputation database that identifies spam sources as they emerge and for as long as they are active. Hosted Email Security informs the sending server that Hosted Email Security is temporarily unavailable by responding with a 450 error (a temporary failure of the requested connection). If the sending server is legitimate, it will try again later.
Hosted Email Security performs this filtering prior to receiving the actual message; therefore the content of the message is not yet scanned.

To manually override IP reputation-based filtering at the MTA connection level, add IP addresses to the lists on the Approved and Blocked IP Addresses screen.

**Tip:**
Hosted Email Security default rules delete all detected viruses, malicious content, phish, and spam.

### 2.1.1.2 General Order of Evaluation

1. **Sender email addresses filtering:**

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

See [Sender Filter Order of Evaluation](#).

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

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

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

See [IP Reputation Order of Evaluation](#).

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

3. **Domain-level policy filtering:**

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

See [Sender Filter Order of Evaluation](#).

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

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

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

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

Evaluation is done in the following order:

1. End User Quarantine website Approved Senders lists
2. Administrator console Approved Senders lists
3. End User Quarantine website Blocked Senders lists
4. Administrator console Blocked Senders lists

2.1.1.4  IP Reputation Order of Evaluation

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

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

The order of evaluation for IP addresses in the lists on the Approved and Blocked IP Addresses screen is based on which list contains the IP address or Classless Inter-Domain Routing (CIDR) block.

Evaluation is done in the following order:

1. The IP Addresses list
   a) On the Approved screen
   b) On the Blocked screen
2. The Country/Region list
   a) On the Approved screen
   b) On the Blocked screen
3. The selected standard IP reputation database lists on the IP Reputation Settings screen
4. The adjusted dynamic IP reputation database lists on the IP Reputation Settings screen
An IP address added to the IP Addresses list on the Approved screen will not be blocked even if that IP address is also in a CIDR block listed on the Blocked screen. Furthermore, that IP address will not be blocked even if it is also in the Known Spam Source standard IP reputation database list.

**Important:**
IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.

2.1.1.5 **Policy Order of Evaluation**

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

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

See [About Rule Actions](#).

Evaluation is done in the following order:

a. "Intercept" actions: Actions in this class intercept the message, preventing it from reaching the original recipient. Intercept actions include deleting the entire message and re-addressing the message.
   
   i. Delete
   
   ii. Deliver Now
   
   iii. Change Recipient
   
   iv. Quarantine

b. "Modify" actions: Actions in this class change the message or its attachments. Modify actions include cleaning cleanable viruses, deleting message attachments, inserting a stamp in the message body, or tagging the subject line.

   i. Cleaning Cleanable Viruses
   
   ii. Deleting Matching Attachments
   
   iii. Tagging the Subject Line
   
   iv. Inserting a Stamp
   
   v. Rule Tokens/Variables

c. "Monitor" actions: Actions in this class allow administrators to monitor messaging. Monitor actions include sending a notification message to others or sending a BCC (blind carbon copy) of the message to others.

   i. Send Notification Action
   
   ii. Bcc Action
d. "Scan Limitation" actions: Actions in this class allow administrators to reject or bypass scanning messages that exceed Hosted Email Security capabilities.
   
   i. Rejecting Messages
   ii. Bypassing Messages

e. "Encrypt Email Message" actions: Actions in this class encrypt the message and then queue it for delivery. This is a non-intercept action, but no other actions can be taken on the target message after this rule is triggered. This action has the lowest priority of all actions, but when triggered it is always the final rule run before the message is queued for delivery. If more than one rule in the rule set is triggered, the rule that uses the encrypt email action will always be triggered last.

### 2.1.2 Outbound Scanning

1. Mail server of example.com will forward the outbound email to Hosted Email Security.

2. Hosted Email Security servers accept the message and perform 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 will be forwarded to outbound MTAs.

4. Outbound MTAs will then route this email to the mail server of the recipient.
2.2 Message Retention

The following table shows message retention information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantined email messages (all regions)</td>
<td>30 days</td>
</tr>
<tr>
<td>Message tracking information</td>
<td>30 days</td>
</tr>
<tr>
<td>Message queue when customer MTA is unavailable</td>
<td>Up to 10 days</td>
</tr>
</tbody>
</table>

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

3.1 Service Requirements

Hosted Email Security does not require hardware on your premises. All scanning is hosted off-site at secure Trend Micro network operations centers. To access your web-based Hosted Email Security administrator console, you need a computer with access to the Internet.

The following are required before Hosted Email Security can be activated:

- An existing mail gateway or workgroup SMTP connection
  For example:
  - A local MTA or mail server
  - A cloud-based MTA solution
- Access to domain MX records (DNS mail exchanger host records) for repointing MX records to the Hosted Email Security MTA
  (Contact your service provider, if necessary, for more information or configuration help.)

3.2 Default Hosted Email Security Settings

To ensure high-quality continuous service and to protect your network from common SMTP attacks such as mail floods and Zip of Death, Hosted Email Security has default settings.

You can find service system limitations by default on the link below:
4 Getting Started

4.1 Registration

1. Contact your Trend Micro sales representative for an Activation Code. An Activation Code uses 37 characters, including hyphens, in the following format:
   XX-XXXX-XXXX-XXXX-XXXX-XXXX

   The Create Account or Sign In screen for the Trend Micro Customer License Portal appears.

   ![Create Account or Sign In](Customer Licensing Portal)

   You are asked, "Do you already have an account?"
3. Select the appropriate option from the following:
   - If you do not already have a Trend Micro Business account, select No, I am a first time user.
   - If you already have a Trend Micro Business account, do the following:
     a. Select Yes, I already have a Trend Micro Business account.
     b. Click Continue.
        The Customer License Portal Sign In appears.

   c. Sign in to your Trend Micro Business account.
      The Enter Your Key screen appears.

4. Type your Hosted Email Security Activation Code.
   Trend Micro sends you an email message with your Customer License Portal sign in information, including
   your account user name, the console web address, and your Activation Code.

5. Start the Hosted Email Security activation process.
### 4.2 Starting the Activation Process

1. Log on to the Hosted Email Security administrator console.  
   
   See [Accessing the Administrator Console](#).

   If no domains are active when you log on to the administrator console, you will go directly to the Service Activation screen. Use this screen to activate the domains you want to manage through Hosted Email Security. To manage domains in Hosted Email Security after activation, see the Administrator's Guide.

2. Type the information for your current MTAs or mail servers in the following fields:
   - Domain name: Includes everything to the right of the at sign (@) in email addresses managed by the server(s) being activated
   - Seat count: Seats correspond to the number of actual email users in the domain
   - Inbound server(s)

   **Note:**
   You can specify up to 30 inbound servers and 30 outbound servers.
   Use the add and the remove buttons to manage additional entries.

   a. IP address or FQDN: Fully qualified domain name (FQDN) is a unique name, which includes both host name and domain name, and resolves to a single IP address.
      
      i. For example: hostmaster1.example.com or mailhost.example.com
      ii. Not valid: example.com

   b. Port: Port is a number from 0-65535 that an inbound server listens on. These ports vary based on server configuration. Well-known ports for email servers include SMTP at 25, SMTPS at 465, and MSA at 587.

   c. Preference: Preference, sometimes referred to as distance, is a value from 1 to 100.

   **Note:**  
   If more than one mail server is available, delivery is prioritized to servers with lower values. Using the same value will balance delivery to each server.

   • Optionally, select Enable outbound filtering and refer to the following table:

   **Warning:**
   Enabling outbound filtering without specifying outbound servers will prevent the delivery of any outbound traffic routed through the service.
## Steps to Configure Outbound Filtering

<table>
<thead>
<tr>
<th>Email Solution</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>You currently use Office 365</td>
<td>Select Use Office 365.</td>
</tr>
<tr>
<td>You currently use Google Apps</td>
<td>Select Use Google Apps.</td>
</tr>
<tr>
<td>You do not use Office 365 or Google Apps</td>
<td>Select Specify IP address(es). Type the IP address(es) of your outbound server(s).</td>
</tr>
</tbody>
</table>

- Send test message to: Optional email address used to confirm email delivery from Hosted Email Security. Manually send test messages from the Domain Management Details screen.

3. **Click Add Domain.**

   If the domain is valid and an MX record for the domain exists, the domain appears in the Domains table at the bottom of the screen.

4. **Click Submit.**

   Trend Micro sends a welcome message to the administrative email address on record confirming that your domain has been added successfully and stating: "This welcome message confirms your domain has been successfully added."

   **Warning:**

   Do not repoint your MX record until you receive the message confirming that your domain has been added. The administrative email address on record should receive the welcome message, which is that confirmation. If you repoint your MX record before your domain has been successfully added, your email messages may be lost.

5. **If you currently use Office 365,** you can configure Office 365 connectors to allow email traffic to or from Hosted Email Security MTAs.

   See [Adding Office 365 Inbound Connectors](#).

   See [Adding Office 365 Outbound Connectors](#).

6. **Finalize your activation.**
4.2.1 Adding Office 365 Inbound Connectors

Before integrating your Microsoft Office 365 managed domain name with Hosted Email Security, perform all steps recommended by Microsoft to complete configuration of Office 365 email management for your domain.

To configure inbound connectors, ensure that you have the following:

- Office 365 administrator account
- Hosted Email Security administrator account
- Office 365 designation server address
- Hosted Email Security welcome email message for created domain
- Mail domain administrator account privileges

Some organizations use Microsoft Office 365 to remotely host their email architecture, allowing Microsoft to manage the day-to-day aspects of maintaining their email servers. Hosted Email Security integrates with Office 365 to provide additional security and benefits.

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

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


1. Log on your Microsoft Office 365 admin center account.
2. In the navigation on the left, go to Service Settings.
3. Under mail flow, click Custom mail rules.
4. In the navigation at the top, go to connectors.
5. Add an Inbound Connector to Office 365.

Configure Office 365 to accept mail filtered by Hosted Email Security for delivery to email accounts in your Office 365 managed domain.

a. Under Inbound Connectors, click the plus icon.
   A new connector configuration screen appears, displaying the general tab.

b. In the Name field, type a descriptive name for the connector.
   For example, type Trend Micro Hosted Email Security.

c. Select Enable inbound connector.

d. Under Connector Type, select Partner.

e. Click save.

f. In the navigation on the left, go to security.

   Under Connection Security, select Opportunistic TLS.
h. Under Domain Restrictions, select None.

i. In the navigation on the left, go to scope.

j. In the Domains field, add your Office 365 managed domain name.
   - For example: example.com
   - Not valid: hostmaster1.example.com or mailhost.example.com

k. In the IP addresses field, add the following Hosted Email Security IP addresses:
   HES IP addresses

l. Click save.

m. Confirm that Enabled is selected for the newly added connector.

4.2.2 Adding Office 365 Outbound Connectors

To configure outbound connectors, ensure that you have the following:

- Office 365 administrator account
- Hosted Email Security administrator account
- Hosted Email Security welcome email message for created domain

Some organizations use Microsoft Office 365 to remotely host their email architecture, allowing Microsoft to manage the day-to-day aspects of maintaining their email servers. Hosted Email Security integrates with Office 365 to provide additional security and benefits.

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

Add an Outbound Connector to Office 365.

Configure Office 365 to relay outbound mail to Hosted Email Security for filtering and delivery to recipients outside of your Office 365 managed domain.

a. Under Outbound Connectors, click the plus icon.
   A new connector configuration screen appears, displaying the general tab.

b. In the Name field, type a descriptive name for the connector.
   For example, type Trend Micro Hosted Email Security.

c. Select Enable outbound connector.

d. Under Connector Type, select Partner.

e. Click save.

f. In the navigation on the left, go to security.

g. Under Connection Security, select Opportunistic TLS.

h. Under Outbound Delivery, select Route mail through smart hosts.
i. In the Domains field, add the FQDN for your Office 365 managed domain name.
   • For example: hostmaster1.example.com or mailhost.example.com
   • Not valid: example.com

j. Under Send domains, add the outbound domains that should be applied to this connector.

   Tip:
   Use an asterisk (*) to include all outbound domains.

k. Click save.

l. Confirm that Enabled is selected for the newly added connector.

4.3 Finalizing Activation

To finalize your activation, point your MX record to the Hosted Email Security MTA for your region.

Trend Micro will not activate your domain until the MX record for your domain points to a Hosted Email Security MTA.

   Warning:
   Do not repoint your MX record until you receive the message confirming that your domain has been added. The administrative email address on record should receive the welcome message, which is that confirmation. If you repoint your MX record before your domain has been successfully added, your email messages may be lost.

1. Point your managed domain MX records to the Hosted Email Security MTA for your region.
   • For Europe, the Middle East, Africa: in.hes.trendmicro.eu
   • For all other regions: in.hes.trendmicro.com

   Tip:
   If your company does not have standardized procedures for pointing MX records, or you would like additional guidance, Trend Micro recommends using the following procedure, which also includes all other steps on this page: See Repointing MX Records (Best Practice).

2. If you added Outbound Servers when you added your domain, configure those servers to relay mail through the following Hosted Email Security MTA for your region:
   • For Europe, the Middle East, Africa: relay.hes.trendmicro.eu
   • For all other regions: relay.hes.trendmicro.com

3. To ensure messages can be received from the Hosted Email Security MTA, configure your firewall to accept email messages only from the following Hosted Email Security IP address / CIDR blocks:
   HES IP addresses
4.3.1 Repointing MX Records (Best Practice)

When activating a domain in Hosted Email Security, Trend Micro recommends making three step-wise changes to your MX record to reduce the chance of security vulnerability or an interruption of service while repointing your MX record.

Before starting the procedure below, optionally learn about MX records.

See: About MX Records and Hosted Email Security

1. Modify the MX record for your domain. Add a pointer to the Hosted Email Security MTA for your region. Set the preference number to the lowest priority/highest distance of all your MTAs.

   **Tip:**
   
   *Preference, sometimes referred to as distance, is a value from 1 to 100. If more than one mail server is available, delivery is prioritized to servers with lower values. Using the same value will balance delivery to each server.*

   *The higher the preference number, the lower the priority of the MX record.*

   - For Europe, the Middle East, Africa: in.hes.trendmicro.eu
     
     <your_domain> MX preference = 20, mail exchanger = <your_domain_mta>
     
     <your_domain> MX preference = 100, mail exchanger = in.hes.trendmicro.eu

   - For all other regions: in.hes.trendmicro.com
     
     <your_domain> MX preference = 20, mail exchanger = <your_domain_mta>
     
     <your_domain> MX preference = 100, mail exchanger = in.hes.trendmicro.com

2. Verify that the status of your domain displays as "Activated" in the administrator console.

   **Tip:**
   
   *DNS propagation can take up to 48 hours. The status of the domain you are adding does not change until DNS propagation is complete. During this time, do not turn off any on-premises security. You may receive some email messages directly for a short time until the transition completes.*

   *While waiting for DNS propagation, you can use the administrator console to customize the domain settings for Policy, Approved Senders, IP Reputation, and Directory Management in the administrator console. See the Administrator's Guide for more information and procedures.*

   a. Log on the administrator console. See Accessing the Administrator Console.

   b. Go to Administration > Domain Management.

   c. In the Domains list, verify that the Status for the domain displays as "Activated".
Tip:
If the status of a domain displays as "Adding" for more than 48 hours, confirm the MX record for that domain is pointed to a Hosted Email Security MTA. Open a command prompt and type one of the following:

For Linux:

dig mx <domain_name>

For Windows:

nslookup -q=mx <domain_name>

When domain status displays as "Activated", the service will begin relaying email to your MTA.

3. Modify the MX record for your domain. Set the preference number for the pointer to the Hosted Email Security MTA for your region to the highest priority/lowest distance of all your MTAs.

Tip:
The lower the preference number, the higher the priority of the MX record.

- For Europe, the Middle East, Africa: in.hes.trendmicro.eu
  <your_domain> MX preference = 20, mail exchanger = <your_domain_mta>
  <your_domain> MX preference = 10, mail exchanger = in.hes.trendmicro.eu

- For all other regions: in.hes.trendmicro.com
  <your_domain> MX preference = 20, mail exchanger = <your_domain_mta>
  <your_domain> MX preference = 10, mail exchanger = in.hes.trendmicro.com

4. To ensure messages can be received from the Hosted Email Security MTA, configure your firewall to accept email messages from all the following Hosted Email Security IP address / CIDR blocks:

HES IP addresses

5. Verify that messages are being delivered from Hosted Email Security. To send a test message using the service, do the following:

a. Log on the administrator console.

b. Go to Administration > Domain Management.

c. In the Domains list, click the newly-added domain name.
   The Domain Information screen appears.

d. In the Send test message to field, type an email address to send a test message to using the service.

e. Click Send.

6. Optionally, customize the domain settings for Policy, Approved Senders, IP Reputation, and Directory Management in the administrator console. See the Administrator's Guide for more information and procedures.
7. If you added Outbound Servers when you added your domain, configure those servers to relay mail through the following Hosted Email Security MTA for your region:

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

8. Modify the MX record for your domain. Delete all entries in the MX record not related to Hosted Email Security. This reduces the chance of spam being sent directly to your mail server.

For Europe, the Middle East, Africa: in.hes.trendmicro.eu
<your_domain> MX preference = 10, mail exchanger = in.hes.trendmicro.eu

For all other regions: in.hes.trendmicro.com
<your_domain> MX preference = 10, mail exchanger = in.hes.trendmicro.com

4.3.2 About MX Records and Hosted Email Security

Tip:
To reduce the chance of a security vulnerability or an interruption of service while repointing your MX record, Trend Micro recommends using the following procedure: Repointing MX Records (Best Practice)

Make sure the MX record is entered exactly as provided in the Hosted Email Security welcome email.

DNS propagation can take up to 48 hours. The status of the domain you are adding does not change until DNS propagation is complete. During this time, do not turn off any on-premise security. You may receive some email messages directly for a short time until the transition completes.

An MX record (DNS mail exchanger host record) determines the message routing for all messages sent to a domain. To route messages destined for your domain through the Hosted Email Security MTA, you must repoint your MX record to the fully qualified domain name (FQDN) provided in the welcome email that Trend Micro sent you after you registered.

To disable Hosted Email Security, point your MX record to route all inbound SMTP traffic to your own mail server.

If you are unsure how to configure the MX records for your domain, contact your Internet Service Provider or your DNS technician.

The following external links to MX record configuration help pages are provided for your convenience:

- GoDaddy

- Network Solutions
  [http://www.networksolutions.com/support/mx-records-mail-servers-2/](http://www.networksolutions.com/support/mx-records-mail-servers-2/)

- Enom
4.4 Accessing the Administrator Console

Access the Hosted Email Security administrator console based on your licensing agreement with Trend Micro. Use one of the following methods:

- Sign in to your Trend Micro Business account using the Customer License Portal (CLP), then access the Hosted Email Security administrator console using the link provided there. See [Using CLP to Access the Administrator Console](#).

- Log on directly to your administrator console at the following web address for your region:
  - For Europe, the Middle East, Africa: https://tm.hes.trendmicro.eu
  - For all other regions: https://tm.hes.trendmicro.com

- Use one of the following authorized Trend Micro reseller credentials to access the administrator console for your managed accounts:
  - For xSP resellers, go to the following web address for your region:
    - For Europe, the Middle East, Africa: https://ui.hes.trendmicro.eu
    - For all other regions: https://ui.hes.trendmicro.com
  - For LMP resellers, substitute your Tenant ID for <tenant-id> in the following web address for your region:
    - For Europe, the Middle East, Africa: https://<tenant-id>.hes.trendmicro.eu
    - For all other regions: https://<tenant-id>.hes.trendmicro.com

4.4.1 Using CLP to Access the Administrator Console

**Tip:**
*When you register, Trend Micro sends you an email message with your Customer License Portal sign in information, including your account user name, the console web address, and your Activation Code.*

1. Go to https://clp.trendmicro.com/FullRegistration?T=TM.
   The Create Account or Sign In screen for the Trend Micro Customer License Portal appears.
2. Select Yes, I already have a Trend Micro Business account.

3. Click Continue.
   The Customer License Portal Sign In appears.

4. Sign in to your Trend Micro Business account.
   The Enter Your Key screen appears.
5. Click Cancel.  
The My Products/Services screen appears.

6. Click Open Console in the box for Hosted Email Security.

7. The Hosted Email Security administrator console appears in a new tab or window.

**Tip:**
Bookmark the address of the administrator console. Use the bookmark to be taken directly to the Hosted Email Security administrator console after signing in to your Trend Micro Business account.

End users can access the Hosted Email Security End-User Quarantine website for self-management. Share the End User Quarantine User’s Guide and the following web address for your region with end users:

For Europe, the Middle East, Africa: [https://euq.hes.trendmicro.eu](https://euq.hes.trendmicro.eu)

For all other regions: [https://euq.hes.trendmicro.com](https://euq.hes.trendmicro.com)
5 Management Console

5.1 Working with the Dashboard

The Dashboard displays charts for email traffic relayed through Hosted Email Security.

The following are the navigation tabs on the Dashboard:

To navigate between the charts, click the tabs.

**Note:**
Data collected within the last 2 hours may not be displayed.
The time zone of the browser accessing Hosted Email Security is used.

Select the data shown in charts and their corresponding thumbnail charts on the Summary tab of the Dashboard using the following controls and settings:

<table>
<thead>
<tr>
<th>Table 1. All Charts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
</tr>
<tr>
<td>---</td>
</tr>
</tbody>
</table>
| Domain and direction of traffic | Select a domain and mail traffic direction using the following controls: 
Managed domain Direction Incoming Refresh 
Tip: 
To select all domains, select all my domains from the Managed domain drop-down list. |
| Time periods | Select a time period at the top of each chart. The following are the definitions of time periods: 
Date: The most recent eight (8) days. Days are split into hours from 0:00 to 23:59. Because days start at midnight, charts with a time period of the current day will never show a full 24 hours of data. 
Week: The most recent eight (8) weeks. Weeks are the days from Sunday to Saturday. Because weeks start on Sunday, charts with a time period of the current week will never show a full seven (7) days of data. 
Month: The most recent two (2) months. Months are days from the first to the last day of the calendar month. Because months start on the first, charts with a time period of the current month will never show the full month of data. 
Last 12 months: The data for the last twelve months plus all days of the current month. |
### Table 1. All Charts

<table>
<thead>
<tr>
<th>Control</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Always shows more than one year of data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The specified time period only affects the data shown on the current chart and its corresponding thumbnail chart on the Summary tab. Changing the selection on a chart does not affect other charts.</td>
</tr>
</tbody>
</table>

---

**Important:**
*Click ➔ Refresh after selecting a new domain under Managed domain, selecting a new direction in the Direction drop-down list, or making any changes to other selections, such as the time period.*

### Table 2. Specific Charts

<table>
<thead>
<tr>
<th>Chart or Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>Select a time period by Date, Week, Month, or Last 12 months to show hourly or daily data for the selected time period.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td></td>
</tr>
<tr>
<td>Threats</td>
<td>Select a time period by Date, Week, Month, or Last 12 months to show the total percentage of messages by value for the selected time period.</td>
</tr>
<tr>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
</tbody>
</table>

| Threats      | Use the Top violators’ drop-down list to select the number of email addresses that display on the chart. |
| Top Spam     |          |
| Top Virus    |          |
| Top Analyzed |          |
| Threats      |          |
| Advanced     |          |
5.1.1 Summary Chart

The Summary tab of the Dashboard provides an overview of data displayed on all other charts in one location. Click on a thumbnail to go to that chart's corresponding tab.
5.1.2 Volume Chart

The Volume tab of the Dashboard displays the total number of accepted and blocked messages and the total percentage of blocked messages.

Select a time period by Date, Week, Month, or Last 12 months to show hourly or daily data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the Summary tab. Changing these selections does not affect other charts.

The traffic direction slightly changes the data displayed on charts. The following is the specific data displayed:

Table 1. Detected Values on Charts

<table>
<thead>
<tr>
<th>Detected Values</th>
<th>For Incoming Mail</th>
<th>For Outgoing Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked</td>
<td>The number of email messages blocked by IP reputation-based filtering at the MTA connection level or by Hosted Email Security incoming security filtering. Possible reasons for blocking include: Recipient address is not resolvable (such as someone@???.com). Spammers forged the mail sender address so the message appears to be coming from the customer domain. The customer's MTA is compromised and is sending spam messages (for example, it is an open relay).</td>
<td></td>
</tr>
<tr>
<td>Accepted</td>
<td>The number of email messages passed by IP reputation-based filtering at the MTA connection level or by Hosted Email Security incoming security filtering.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The number of messages passed by Hosted Email Security relay mail service filtering.</td>
<td></td>
</tr>
</tbody>
</table>
Table 1. Detected Values on Charts

<table>
<thead>
<tr>
<th>Detected Values</th>
<th>For Incoming Mail</th>
<th>For Outgoing Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked %</td>
<td>The percentage of email messages blocked by IP reputation-based filtering at the MTA connection level or by Hosted Email Security incoming security filtering</td>
<td>The percentage of messages blocked by Hosted Email Security relay mail service filtering</td>
</tr>
<tr>
<td>Total</td>
<td>The total number of email messages processed</td>
<td></td>
</tr>
</tbody>
</table>

5.1.3 Bandwidth Chart

The Bandwidth tab of the Dashboard displays the total size of email messages accepted in KB.

Select a time period by Date, Week, Month, or Last 12 months to show hourly or daily data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the Summary tab. Changing these selections does not affect other charts.

The traffic direction does not change the data displayed on charts. The following is the specific data displayed:
Table 1. Detected Values on Charts

<table>
<thead>
<tr>
<th>Detected Values</th>
<th>For Incoming Mail</th>
<th>For Outgoing Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Quarantined</td>
<td>The total size of email messages that Hosted Email Security did not quarantine</td>
<td></td>
</tr>
<tr>
<td>Quarantined</td>
<td>The total size of email messages that Hosted Email Security quarantined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: By default, no messages are quarantined. To begin using the quarantine, select a quarantine action for one or more policy rules.</td>
<td></td>
</tr>
<tr>
<td>Total Size</td>
<td>The total size of email messages scanned by Hosted Email Security</td>
<td></td>
</tr>
</tbody>
</table>

5.1.4 Threats Chart

The Threats tab of the Dashboard displays the total percentage of messages detected as threats.

Select a time period by Date, Week, Month, or Last 12 months to show the total percentage of messages by value for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the Summary tab. Changing these selections does not affect other charts.

The traffic direction slightly changes the data displayed on charts. The following is the specific data displayed:
### Table 1. Detected Values on Charts

<table>
<thead>
<tr>
<th>Detected Values</th>
<th>For Incoming Mail</th>
<th>For Outgoing Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blocked</strong></td>
<td>The number of email messages blocked by IP reputation-based filtering at the MTA connection level or by Hosted Email Security incoming security filtering. <strong>Note:</strong> This value does not include messages blocked by content-based filtering.</td>
<td>The number of messages blocked using Hosted Email Security relay mail service filtering. Possible reasons for blocking include: Recipient address is not resolvable (such as someone@???.com). Spammers forged the mail sender address so the message appears to be coming from the customer domain. The customer’s MTA is compromised and is sending spam messages (for example, it is an open relay).</td>
</tr>
<tr>
<td><strong>Virus</strong></td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as containing a malware threat.</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as containing a malware threat.</td>
</tr>
<tr>
<td>** Analyzed Advanced Threats**</td>
<td>The number of email messages containing suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection and detected as high-risk using advanced analysis.</td>
<td>Not available.</td>
</tr>
<tr>
<td><strong>Probable Advanced Threats</strong></td>
<td>The number of email messages containing suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection but not analyzed using advanced analysis.</td>
<td>Not available.</td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
<td>The number of email messages containing URL of sites that directly or indirectly facilitate the distribution of ransomware.</td>
<td>The number of email messages containing URL of sites that directly or indirectly facilitate the distribution of ransomware.</td>
</tr>
<tr>
<td><strong>Phish</strong></td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as phishing threats.</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as phishing threats.</td>
</tr>
<tr>
<td><strong>Spam</strong></td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as spam. <strong>Note:</strong> Hosted Email Security includes messages detected as marketing messages in the &quot;Spam&quot; category.</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as spam.</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td>The number of email messages detected by content-based policy rules (for example, attachment true file type).</td>
<td>The number of email messages detected by content-based policy rules (for example, attachment true file type).</td>
</tr>
<tr>
<td><strong>Clean</strong></td>
<td>The number of email messages that passed IP reputation-based and content-based.</td>
<td>The number of mail messages that passed Hosted Email Security relay mail service.</td>
</tr>
</tbody>
</table>
Table 1. Detected Values on Charts

<table>
<thead>
<tr>
<th>Detected Values</th>
<th>For Incoming Mail</th>
<th>For Outgoing Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>filtering</td>
<td>filtering</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>The total number of email messages processed</td>
<td></td>
</tr>
</tbody>
</table>

5.1.5 Threats Details Chart

The Threat Details tab of the Dashboard displays the number of messages detected as threats and the total percentage of blocked messages.

For a summary of the total number of email messages scanned by detected category, refer to the table at the bottom of the Threat Details tab. This table is not shown in the thumbnail view on the Summary screen.
Select a time period by Date, Week, Month, or Last 12 months to show hourly or daily data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the Summary tab. Changing these selections does not affect other charts.

The traffic direction slightly changes the data displayed on charts. The following is the specific data displayed:

<table>
<thead>
<tr>
<th>Detected Values</th>
<th>For Incoming Mail</th>
<th>For Outgoing Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked</td>
<td>The number of email messages blocked by IP reputation-based filtering at the MTA connection level or by Hosted Email Security incoming security filtering.</td>
<td>The number of messages blocked using Hosted Email Security relay mail service filtering. Possible reasons for blocking include: Recipient address is not resolvable (such as someone@???.com). Spammers forged the mail sender address so the message appears to be coming from the customer domain. The customer’s MTA is compromised and is sending spam messages (for example, it is an open relay).</td>
</tr>
<tr>
<td>Note: This value does not include messages blocked by content-based filtering.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as containing a malware threat.</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as containing a malware threat.</td>
</tr>
<tr>
<td>Analyzed Advanced Threats</td>
<td>The number of email messages containing suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection and detected as high-risk using advanced analysis.</td>
<td>Not available</td>
</tr>
<tr>
<td>Probable Advanced Threats</td>
<td>The number of email messages containing suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection but not analyzed using advanced analysis.</td>
<td>Not available</td>
</tr>
<tr>
<td>Ransomware</td>
<td>The number of email messages containing URL of sites that directly or indirectly facilitate the distribution of ransomware.</td>
<td>The number of email messages containing URL of sites that directly or indirectly facilitate the distribution of ransomware.</td>
</tr>
<tr>
<td>Phish</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as phishing threats.</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as phishing threats.</td>
</tr>
<tr>
<td>Spam</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as spam.</td>
<td>The number of email messages that Hosted Email Security content-based filtering detected as spam.</td>
</tr>
</tbody>
</table>
### Table 1. Detected Values on Charts

<table>
<thead>
<tr>
<th>Detected Values</th>
<th>For Incoming Mail</th>
<th>For Outgoing Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Hosted Email Security includes messages detected as marketing messages in the &quot;Spam&quot; category.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>The number of email messages detected by content-based policy rules (for example, attachment true file type)</td>
<td>The number of email messages detected by content-based policy rules (for example, attachment true file type)</td>
</tr>
<tr>
<td>Clean</td>
<td>The number of email messages that passed IP reputation-based and content-based filtering</td>
<td>The number of mail messages that passed Hosted Email Security relay mail service filtering</td>
</tr>
<tr>
<td>Total</td>
<td>The total number of email messages processed</td>
<td></td>
</tr>
</tbody>
</table>

### 5.1.6 Advanced Analysis Details Chart

The Advanced Analysis Details tab of the Dashboard displays the number and level of threats detected by the advanced analysis based on the selected mail traffic direction.

**Note:** The data on this tab is displayed for incoming mail traffic only.

For a summary of the total number of email messages scanned by detected category, refer to the table at the bottom of the Threat Details tab. This table is not shown in the thumbnail view on the Summary screen.
5.1.7 Top Spam Chart

The Top Spam tab of the Dashboard displays the email addresses that sent or received the most spam messages based on the selected mail traffic direction.

Hover over a bar to see details.
Select a time period by Date, Week, or Month to show hourly or daily data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the Summary tab. Changing these selections does not affect other charts.

Use the Top violators drop-down list to select the number of email addresses that display on the chart.

5.1.8 Top Virus Chart

The Top Virus tab of the Dashboard displays the email addresses that sent or received the most messages containing malware threats based on the selected mail traffic direction.

Hover over a bar to see details.
Select a time period by Date, Week, or Month to show hourly or daily data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the Summary tab. Changing these selections does not affect other charts.

Use the Top violators drop-down list to select the number of email addresses that display on the chart.

### 5.1.9 Top Analyzed Advanced Threats

The Top Analyzed Advanced Threats tab of the Dashboard displays the email addresses that received the most messages containing advanced threats based on the selected mail traffic direction.

**Note:**
The data on this tab is displayed for incoming mail traffic only.

Hover over a bar to see details.
Select a time period by Date, Week, or Month to show hourly or daily data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the Summary tab. Changing these selections does not affect other charts.

Use the Top violators drop-down list to select the number of email addresses that display on the chart.
5.2 Configuring a Policy

The Policy screen shows a list of the currently defined rules and their status. From this screen you can add a new rule and edit, copy, or delete existing rules.

The rules are displayed in a table, sorted by the order in which the rules are applied during scanning by Hosted Email Security. You can filter the information by using the drop-down lists at the top.

<table>
<thead>
<tr>
<th>Table 1. Policy Terminology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
</tr>
<tr>
<td>Rules</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>Order</td>
</tr>
<tr>
<td>Modified</td>
</tr>
<tr>
<td>Last Used</td>
</tr>
<tr>
<td>Status</td>
</tr>
</tbody>
</table>

5.2.1 Managing Policy Rules

Hosted Email Security offers content-based filtering at the message level. Rules are the means by which messaging policies are applied to message traffic in Hosted Email Security. At any time, an administrator can see the rules that apply to their organization, and can make changes to the rules that comprise their policy, rename those rules, and create new rules. Each rule can be disabled if desired without losing its definition, and re-enabled at a later time.

<table>
<thead>
<tr>
<th>Table 1. Policy Rule Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
</tr>
<tr>
<td>Adding Policy Rules</td>
</tr>
<tr>
<td><strong>Tip:</strong> Often a new rule will be very similar to one you already have. In that case, it is usually easier to copy the rule and edit it rather than create a new rule from scratch.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Table 1. Policy Rule Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copying Policy Rules</td>
<td>In the Rules list, select the rule to copy. Click Copy.</td>
</tr>
<tr>
<td>Editing Policy Rules</td>
<td>In the Rules list, click the name of the rule you want to edit and follow the selection procedures in <a href="#">Adding Policy Rules</a>.</td>
</tr>
<tr>
<td>Deleting Policy Rules</td>
<td>In the Rules list, select the rule or rules to delete. Click Delete.</td>
</tr>
</tbody>
</table>

#### 5.2.2 Selecting User Accounts for Rules

Configuring sender, recipient, and exclusion lists with specific users and groups is done using this screen. Its appearance differs slightly depending on which direction the messages are routed and whether Sender or Recipient addresses are being selected.

1. (For outgoing messages for Recipients and incoming messages for Senders only) Choose one of the following:
   - Anyone to select any email addresses at all.
   - Selected addresses.

2. From the drop-down list, select a means of adding selected addresses.
   - My domains populate a list box below with the available domains.
   - My groups populate a list box below with the available groups.
   - Type address or domain provides a text entry field.

3. (For My Domains or My groups option) Select any desired domains or groups from that display and click Add. The selected items are copied to the selected list at the right.

4. (For Type address or domain option) Type a specific domain or wildcarded address in the field and click Add.

5. Click Save when the selected list includes all the user groups, domains, and addresses that you want in it.

#### 5.2.3 About Rule Target Criteria

Rule criteria allow you to specify the conditions that the rule applies to messages scanned by Hosted Email Security.

The available criteria are shown in a list in the center of the screen. Some of these criteria have links to screens where you specify the associated details.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>No criteria</td>
<td>All messages</td>
</tr>
<tr>
<td>Message contains</td>
<td>&quot;viruses or malicious code&quot;</td>
</tr>
<tr>
<td>Message detected as</td>
<td>&quot;Spam&quot;</td>
</tr>
<tr>
<td></td>
<td>Detected viruses, worms, and other threats.</td>
</tr>
<tr>
<td></td>
<td>Detected spam.</td>
</tr>
</tbody>
</table>
Table 1. Basic Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Phish&quot;</td>
<td>Detected phish.</td>
</tr>
<tr>
<td>&quot;Marketing message&quot;</td>
<td>Detected marketing message.</td>
</tr>
<tr>
<td>&quot;Social engineering attack&quot;</td>
<td>Detected social engineering attack.</td>
</tr>
</tbody>
</table>

Advanced

**Note:** Select Advanced to display the "Advanced" criteria.

- "All Match"
- "Any Match"

Specific attribute and content targets
See Configuring Advanced Criteria.

5.2.3.1 Configuring Virus or Malicious Code Criteria

The Message contains "viruses or malicious code" criteria allow you to create rules that take actions on messages that contain viruses, worms, or other malicious code.

1. Select Message contains.

2. Click the viruses or malicious code link on the Rule > Criteria screen.
   The Viruses or Malicious Code screen appears.

3. To perform scanning for less conventional threats, select Enable Advanced Threat Scan Engine.
   See About Advanced Threat Scan Engine.

   - Select Perform advanced analysis to identify threats, and then select the threat level from the drop-down list, to perform further observation and analysis for threats detected by the Advanced Threat Scan Engine.

   - Select Include macro scanning during advanced analysis to include macro threats during observation and analysis.

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

Hosted Email Security logs advanced threats as follows:

- "Probable Advanced Threats": Suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection but not analyzed using advanced analysis

**Tip:** Some detected files may be safe. Trend Micro recommends selecting the Quarantine action for suspected threats detected by the Advanced Threat Scan Engine.
• "Analyzed Advanced Threats": Suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection using advanced analysis

**Note:**
The Advanced Threat Scan Engine or Social Engineering Attack Protection consider messages as suspected threats according to the security level configured for advanced analysis. That is:

- if the High security level is configured for advanced analysis, then the action will be applied on all messages that exhibit any suspicious behavior.

- if the Medium security level is configured for advanced analysis, then the action will be applied on messages that have moderate to high probability of being malicious.

- if the Low security level is configured for advanced analysis, then the action will be applied only on messages that have high probability of being malicious.

4. Specify at least one of the following detection types.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cleanable viruses or malicious code</td>
<td>Apply the rule to messages or attachments that contain cleanable viruses. Cleanable viruses are those that can be safely removed from the contents of the infected file, resulting in an uninfected copy of the original message or attachment.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> Selecting Cleanable viruses or malicious code as rule criteria, and then selecting a rule action other than Delete or Clean, can result in infected messages or attachments entering your messaging environment. By default, Hosted Email Security is configured with virus rules to appropriately handle threats when it is installed.</td>
</tr>
<tr>
<td>Uncleanables with mass-mailing behavior</td>
<td>Apply the rule to messages that contain uncleanable viruses, worms, or other threats that cannot be removed from messages or attachments, and that propagate by mass-mailing copies of themselves.</td>
</tr>
<tr>
<td>Uncleanables without mass-mailing behavior</td>
<td>Select the categories below as desired:</td>
</tr>
<tr>
<td></td>
<td>• Spyware</td>
</tr>
<tr>
<td></td>
<td>• Dialers</td>
</tr>
<tr>
<td></td>
<td>• Hacking tools</td>
</tr>
<tr>
<td></td>
<td>• Password cracking applications</td>
</tr>
<tr>
<td></td>
<td>• Adware</td>
</tr>
<tr>
<td></td>
<td>• Joke programs</td>
</tr>
<tr>
<td></td>
<td>• Remote access tools</td>
</tr>
<tr>
<td></td>
<td>• All others</td>
</tr>
</tbody>
</table>
5.2.3.1  About Advanced Threat Scan Engine

The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.

Major features include:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities
- Enhanced parsers for handling file deformities

**Important:**
*Because ATSE identifies both known and unknown advanced threats, enabling ATSE may increase the possibility of legitimate files being flagged as malicious.*

5.2.3.2  Configuring Spam Criteria

The Spam, Phish, Marketing message, or Social engineering attack criteria allow you to create rules that take actions on these types of potentially unwanted messages.

**Note:**
*Hosted Email Security does not apply content-based heuristic spam, phish, marketing message, or social engineering attack rules to email messages received from email addresses and domains listed on the Approved Senders screen.*

1. Select Message detected as.
2. Select "Spam".
3. Choose a baseline spam catch rate.

   - Lowest (most conservative)
   - Low
   - Moderately low
   - Moderately high
   - High
   - Highest (most aggressive)
5.2.3.3 Configuring Phish Criteria

The Spam, Phish, Marketing message, or Social engineering attack criteria allow you to create rules that take actions on these types of potentially unwanted messages.

**Note:**
Hosted Email Security does not apply content-based heuristic spam, phish, marketing message, or social engineering attack rules to email messages received from email addresses and domains listed on the Approved Senders screen.

1. Select Message detected as.
2. Select "Phish and other suspicious content".

5.2.3.4 Configuring Marketing Message Criteria

Marketing messages are email messages that have commercial or fund-raising content that the user may have requested, but that often do not include an opt-out option.

The Spam, Phish, Marketing message, or Social engineering attack criteria allow you to create rules that take actions on these types of potentially unwanted messages.

**Note:**
Hosted Email Security does not apply content-based heuristic spam, phish, marketing message, or social engineering attack rules to email messages received from email addresses and domains listed on the Approved Senders screen.

1. Select Message detected as.
2. Select "Marketing message".
3. To omit the IP addresses of specific mail servers from this rule, select Exception list. The Marketing Message Exception List screen appears.

**Note:**
The rule will not apply to marketing messages from IP addresses in this exception list. The list is specific just to the rule being edited.

5.2.3.5 Configuring Social Engineering Attack Criteria

Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages.

For more information about social engineering attack detections, see [Social Engineering Attack Log Details](#).

The Spam, Phish, Marketing message, or Social engineering attack criteria allow you to create rules that take actions on these types of potentially unwanted messages.
1. Select Message detected as.

2. Select Social engineering attack.

   • Select Perform advanced analysis to identify threats, and then select the threat level from the drop-down list, to perform further observation and analysis for threats detected by Social Engineering Attack Protection.

   **Note:** hosted email security does not apply content-based heuristic spam, phish, marketing message, or social engineering attack rules to email messages received from email addresses and domains listed on the Approved Senders screen.

Hosted Email Security logs advanced threats as follows:

   • "Probable Advanced Threats": Suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection but not analyzed using advanced analysis

   **Tip:** Some detected files may be safe. Trend Micro recommends selecting the Quarantine action for suspected threats detected by Social Engineering Attack Protection.

   • "Analyzed Advanced Threats": Suspected threats detected by the Advanced Threat Scan Engine or Social Engineering Attack Protection using advanced analysis

   **Note:** The Advanced Threat Scan Engine or Social Engineering Attack Protection considers messages as suspected threats according to the security level configured for advanced analysis. That is:

   • if the High security level is configured for advanced analysis, then the action will be applied on all messages that exhibit any suspicious behavior.

   • if the Medium security level is configured for advanced analysis, then the action will be applied on messages that have moderate to high probability of being malicious.

   • if the Low security level is configured for advanced analysis, then the action will be applied only on messages that have high probability of being malicious.
5.2.3.6 Configuring Advanced Criteria

On the Criteria screen, select Advanced to display the advanced criteria.

Do one of the following:

- Select "All Match" to the right of Advanced to trigger the rule only when all selected "Advanced" criteria are matched.

- Select "Any Match" to the right of Advanced to do the following:
  - Trigger the rule when any selected "Advanced" criteria are matched
  - Display the Attachment is "password protected" and Recipient number criteria in the "Advanced" criteria list

| Attachment content matches | "keyword expressions"
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment size is</td>
<td>&gt; ▼ 5 MB ▼</td>
</tr>
<tr>
<td>Attachment number is</td>
<td>&gt; ▼ 20</td>
</tr>
<tr>
<td>Attachment is</td>
<td>&quot;password protected&quot;</td>
</tr>
<tr>
<td>Recipient number</td>
<td>&gt; ▼ 0</td>
</tr>
</tbody>
</table>

The following tables all contain the same information sorted differently. Use the following sorted tables to find appropriate "Advanced" criteria to filter messages by your desired rule targets:

Table 1. Advanced Criteria Sorted by Display Order

<table>
<thead>
<tr>
<th>Rule Targets</th>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment is</td>
<td>&quot;name or extension&quot; &quot;</td>
<td>Attachment name or extension</td>
</tr>
<tr>
<td>Attachment is</td>
<td>&quot;MIME content-type&quot; &quot;</td>
<td>Attachment MIME content-type</td>
</tr>
<tr>
<td>Attachment is</td>
<td>&quot;true file type&quot;</td>
<td>Attachment true file type</td>
</tr>
<tr>
<td>Message size is</td>
<td>&gt;, &lt;= &lt;number&gt; KB, MB</td>
<td>Size</td>
</tr>
<tr>
<td>Subject matches</td>
<td>&quot;keyword expressions&quot;</td>
<td></td>
</tr>
<tr>
<td>Subject is</td>
<td>&quot;blank&quot;</td>
<td>Keywords in headers and content</td>
</tr>
<tr>
<td>Body matches</td>
<td>&quot;keyword expressions&quot;</td>
<td></td>
</tr>
<tr>
<td>Specified header matches</td>
<td>&quot;keyword expressions&quot;</td>
<td></td>
</tr>
<tr>
<td>Attachment content matches</td>
<td>&quot;keyword&quot;</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1. Advanced Criteria Sorted by Display Order

<table>
<thead>
<tr>
<th>Rule Targets</th>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>expressions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot; greater, less than or equal to number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attachment number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot; password protected &quot;</td>
</tr>
<tr>
<td>Attachment is</td>
<td>&gt;, &lt;= &lt;number&gt; B, KB, MB</td>
<td></td>
</tr>
<tr>
<td>Attachment number is</td>
<td>&gt;, &lt;= &lt;number&gt;</td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>Select &quot;Any Match&quot; to the right of Advanced to display these criteria.</td>
<td></td>
</tr>
<tr>
<td>Recipient number</td>
<td>&gt;, &lt;= &lt;number&gt;</td>
<td>Number of recipients</td>
</tr>
<tr>
<td>Note:</td>
<td>Select &quot;Any Match&quot; to the right of Advanced to display these criteria.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 2. Advanced Criteria Sorted by Attribute and Content Targets

<table>
<thead>
<tr>
<th>Rule Targets</th>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and type attributes</td>
<td>Attachment is</td>
<td>&quot; name or extension &quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot; MIME content-type &quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot; true file type &quot;</td>
</tr>
<tr>
<td>Size attributes</td>
<td>Message size is</td>
<td>&gt;, &lt;= &lt;number&gt; KB, MB</td>
</tr>
<tr>
<td></td>
<td>Attachment size is</td>
<td>&gt;, &lt;= &lt;number&gt; B, KB, MB</td>
</tr>
<tr>
<td>Keyword content</td>
<td>Subject matches</td>
<td>&quot; keyword expressions &quot;</td>
</tr>
<tr>
<td></td>
<td>Subject is</td>
<td>&quot; blank &quot;</td>
</tr>
<tr>
<td></td>
<td>Body matches</td>
<td>&quot; keyword expressions &quot;</td>
</tr>
<tr>
<td></td>
<td>Specified header matches</td>
<td>&quot; keyword expressions &quot;</td>
</tr>
</tbody>
</table>
### Table 2. Advanced Criteria Sorted by Attribute and Content Targets

<table>
<thead>
<tr>
<th>Rule Targets</th>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment content matches</td>
<td>&quot;keyword expressions&quot;</td>
<td></td>
</tr>
<tr>
<td>Attachment number is</td>
<td>&gt;, &lt;= &lt;number&gt;</td>
<td>Number of attachments</td>
</tr>
<tr>
<td>Recipient number</td>
<td>&gt;, &lt;= &lt;number&gt;</td>
<td>Number of recipients</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select &quot;Any Match&quot; to the right of Advanced to display these criteria.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select &quot;Any Match&quot; to the right of Advanced to display these criteria.</td>
<td></td>
</tr>
<tr>
<td>Attachment is</td>
<td>&quot;password protected&quot;</td>
<td>Zipped, signed, or password-protected attachment</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select &quot;Any Match&quot; to the right of Advanced to display these criteria.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 3. Advanced Criteria Sorted by Message-Only or Attachment-Only Targets

<table>
<thead>
<tr>
<th>Rule Targets</th>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size is</td>
<td>&gt;, &lt;= &lt;number&gt; KB, MB</td>
<td>Size</td>
</tr>
<tr>
<td>Subject matches</td>
<td>&quot;keyword expressions&quot;</td>
<td></td>
</tr>
<tr>
<td>Subject is</td>
<td>&quot;blank&quot;</td>
<td>Keywords in headers and content</td>
</tr>
<tr>
<td>Body matches</td>
<td>&quot;keyword expressions&quot;</td>
<td></td>
</tr>
<tr>
<td>Specified header matches</td>
<td>&quot;keyword expressions&quot;</td>
<td></td>
</tr>
<tr>
<td>Recipient number</td>
<td>&gt;, &lt;= &lt;number&gt;</td>
<td>Number of recipients</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select &quot;Any Match&quot; to the right of Advanced to display these criteria.</td>
<td></td>
</tr>
<tr>
<td>Attachment-only</td>
<td>Attachment is</td>
<td>Attachment name or extension</td>
</tr>
<tr>
<td></td>
<td>&quot;name or extension&quot;</td>
<td>Attachment MIME content-type</td>
</tr>
<tr>
<td></td>
<td>&quot;MIME content-type&quot;</td>
<td>Attachment true file type</td>
</tr>
<tr>
<td></td>
<td>&quot;true file type&quot;</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3. Advanced Criteria Sorted by Message-Only or Attachment-Only Targets

<table>
<thead>
<tr>
<th>Rule Targets</th>
<th>Criteria</th>
<th>Filter Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment content matches</td>
<td>&quot; keyword expressions &quot;</td>
<td>Keywords in headers and content</td>
</tr>
<tr>
<td>Attachment size is</td>
<td>&gt;, &lt;= &lt;number&gt; B, KB, MB</td>
<td>Attachment size</td>
</tr>
<tr>
<td>Attachment number is</td>
<td>&gt;, &lt;= &lt;number&gt;</td>
<td>Number of attachments</td>
</tr>
<tr>
<td>Attachment is</td>
<td>&quot; password protected &quot;</td>
<td>Zipped, signed, or password-protected attachment</td>
</tr>
</tbody>
</table>

**Note:** Select "Any Match" to the right of Advanced to display these criteria.

### 5.2.3.6.1 About Keyword Expressions

Keyword expressions can be:

- Groups of literal text characters
- Patterns, defined using symbols (regular expressions) that describe a range of possible groupings of text
- A mixture of literal text and symbolic patterns

For example, a keyword expression might be a single word, a phrase, or even a substring; or it might be a pattern that defines a more general grouping of text, such as an asterisk used as a wildcard to stand in for any text of one or more characters in length.

Regular expressions, often called regexes, are sets of symbols and syntactic elements used to match patterns of text. The symbols stand in for character patterns or define how the expression is to be evaluated. Using regular expressions is sophisticated way to search for complex character patterns in large blocks of text. For example, suppose you want to search for the occurrence of an email address—any email address—in a block of text. You can build a regular expression that will match any pattern of text that has any valid name string, followed by an @ character, followed by any valid domain name string, followed by a period, followed by any valid domain suffix string.

Hosted Email Security uses a subset of POSIX regular expression syntax. For a few simple examples, see Regular Expression Examples.

**Tip:**

*If your expression includes the characters \ | ( ) { } [ ] ^ $ * + ?, you must escape them by using a \ immediately before the character. Otherwise, they will be assumed to be regular expression operators rather than literal characters.*
This help system contains a brief summary of common regex elements, but a thorough guide to regular expression syntax is beyond the scope of this help system. However, there are many sources of reference information available on the Web or in books.

5.2.3.6.1.1  Using Keyword Expressions

You can select existing keyword expressions from the list of those available. New keyword expressions can be defined and saved, either from scratch or by copying and editing an existing expression.

1. Select an existing keyword expression from the Available field.

2. Click the move button (Add>) to move the selected keyword expression to the Selected field.

   Note:
   You can also add, edit, copy, or delete keyword expressions.

3. Repeat until you have moved all the keyword expressions you want to apply.

5.2.3.6.1.2  Adding Keyword Expressions

New keyword expressions can be defined and saved, and then applied to a rule.

1. Click Add.

2. Type a name for the list.

3. Select Match criteria:

   - Select Any specified to match keywords based on a logical OR.
   - Select All specified to match keywords based on a logical AND.
   - Select Not the specified to apply the rule to messages that do not contain the keywords.

4. Click on individual keyword expressions in the list below to edit them.

5. Repeat until you have added your keyword expressions to the list.

5.2.3.6.1.3  Editing Keyword Expressions

Existing keyword expressions can be modified, or can be copied with a new name.

1. Click Edit.

2. Edit the Match criteria if desired:

   - Select Any specified to match keywords based on a logical OR.
   - Select All specified to match keywords based on a logical AND.
   - Select Not the specified to apply the rule to messages that do not contain the keywords.

3. Click on individual keyword expressions in the list below to edit them.
Using Attachment Name or Extension Criteria

The Attachment is "name or extension" criteria allows you to create rules that take actions on messages based on the name or the extension of attachments a message contains.

1. On the Criteria screen, select Advanced to display the advanced criteria.

2. Select the Attachment is "name or extension" criteria.

3. Click the "name or extension" link.
   The Attachment Names screen appears.

4. From the drop-down list, select either Selected attachment names or not the selected attachment names.

5. If you want to block attachment names by file extension:
   a. Select File extensions to block (recommended) and/or File extensions to block (commonly exchanged).

   **Note:**
   The "recommended" category contains those whose file types commonly act as containers for malware and are not types that are normally exchanged via email in an organization. This list includes extensions such as COM, DLL, and EXE. The commonly exchanged category includes file types that are commonly sent between members of an organization.

   The latter list includes the DOC extension used by Microsoft Word documents. These files are often used to propagate VB macro viruses, but they are also often commonly exchanged within organizations.

   b. Click the open arrow buttons to drop-down the lists of standard file extensions.

   c. Select the file extensions for Hosted Email Security to trigger on for this rule.

   d. Click the close arrow button to collapse the list.

6. If you want to block attachments with your own specified names or extensions:
   a. Select Attachments named.

   b. Type an extension to block or use an asterisk (*) as a substitute for any part of a filename.

   **Tip:**
   The following examples are valid:
   
   - doc or *.doc
   - docx or *.docx
   - doc* or *.doc*
   - LOVE-LETTER-FOR-YOU.TXT.vbs
   - LOVE-LETTER*.vbs

   c. Click Add.
      The file name is added to the list just below.
 Tip: If there are any names in the list that you want to delete, select them and click Delete.

5.2.3.6.3 Using Attachment MIME Content-type Criteria

The Attachment is "MIME content-type" criteria allow you to create rules that take actions on messages based on the MIME content-type of attachments a message contains.

Note: Where the Attachment is "MIME content-type" criteria makes decisions based on the MIME content-type indicated, the Attachment is "true file type" criteria scans the headers of the actual attached files themselves for the identifying signatures.

1. On the Criteria screen, select Advanced to display the advanced criteria.
2. Select the Attachment is "MIME content-type" criteria.
3. Click the "MIME content-type" link.
   The Attachment MIME screen appears.
4. From the drop-down list, select either Selected attachment names or Not the selected attachment names.
5. Select the MIME types for Hosted Email Security to match on.
6. If you want to block attachments by explicit MIME content-types:
   a. Select Other MIME content-type.
   b. Type the names of the MIME content-types to block.

Tip: The following examples are valid:
   - 3dm or *.3dm
   - 3dmf or *.3dmf

Tip: If there are any names in the list that you want to delete, select them and click Delete.

5.2.3.6.4 Using Attachment True File Type Criteria

The Attachment is "true file type" criteria allows you to create rules that take actions on messages based on the true file type of attachments a message contains.

Note: Where the Attachment is "name or extension" criteria makes decisions based on just filenames and/or extensions, the Attachment is "true file type" criteria scans the headers of the files themselves for the identifying signatures.
1. On the Criteria screen, select Advanced to display the advanced criteria.

2. Select the Attachment is "true file type" criteria.

3. Click the "true file type" link.
   a) The Attachment True File Type screen appears.

4. From the drop-down list, select selected attachment types or Not the selected attachment types.

5. Select the true file types for Hosted Email Security to match on.

   ![Note]
   The Compressed file type of other includes only the following file types: ar, arc, amg, lzw, cab, lha, pklite, diet, lzh, and lz.

   5.2.3.6.5 Using Message Size Criteria
1. On the Criteria page, select Advanced to display the advanced criteria.

2. Select Message size is in the criteria list.

3. Select > or <= from the comparison drop-down list.
   • Select > to apply the rule to messages that are larger than the specified size.
   • Select <= to apply the rule to messages that are smaller than or equal to the specified size.

   For example, <= 10 MB applies the rule to all messages that are smaller than or equal to 10 megabytes.

4. Type a number for the size.

5. Select a unit of measurement from the following choices:
   • KB: Kilobytes
   • MB: Megabytes

   ![Note]
   The Message size is a criteria applied to the total size of a message, including any attachments it might contain.

   For example, if a message contained two attachments, one a 3 MB attachment and the other a 1 MB attachment, a rule that deletes messages over 2 MB would delete the entire message, including both attachments.

   5.2.3.6.6 Using Subject Matches Criteria

   Hosted Email Security can scan the message subject for keyword expressions.

   1. On the Criteria screen, select Advanced to display the advanced criteria.

   2. Select Subject matches “keyword expressions”.

   3. Click the "keyword expressions" link.

   4. Configure keywords.
5.2.3.6.7 Using Subject is Blank Criteria

Hosted Email Security can scan the message for a blank subject line.

1. On the Criteria screen, select Advanced to display the advanced criteria.
2. Select Subject is "blank".

5.2.3.6.8 Using Body Matches Criteria

Hosted Email Security can scan the message body for keyword expressions.

1. On the Criteria screen, select Advanced to display the advanced criteria.
2. Select Body matches.
3. Click the "keyword expressions" link.
4. Configure keywords.

5.2.3.6.9 Using Specified Header Matches Criteria

Hosted Email Security can scan the message headers for keyword expressions.

1. On the Criteria screen, select Advanced to display the advanced criteria.
2. Select Specified header matches.
3. Click the "keyword expressions" link.
4. Configure keywords.

5.2.3.6.10 Using Attachment Content Matches Keyword Criteria

The Attachment content matches "keyword expressions" criteria allows you to create rules that take actions on messages based on keyword expressions contained in a message.

1. On the Criteria screen, select Advanced to display the advanced criteria.
2. Select the Attachment content matches "keyword expressions" criteria.
3. Click the "keyword expressions" link.
The Attachment Content Keyword Expressions screen appears.
4. Configure the keywords.

5.2.3.6.11 Using Attachment Size Criteria

The Attachment size is criteria allows you to create rules that take actions on messages based on the size of any attachments to the message.

1. On the Criteria screen, select Advanced to display the advanced criteria.
2. Select the Attachment size is criteria.

3. Select > or <= from the comparison drop-down list.
   - Select > to apply the rule to attachments that are larger than the specified size.
   - Select <= to apply the rule to attachments that are smaller than or equal to the specified size.

   For example, <= 10 MB applies the rule to all messages that are equal to or smaller than 10 megabytes.

4. Type a value for the size.

5. Select a unit of measurement from the following choices:
   - B: Bytes
   - KB: Kilobytes
   - MB: Megabytes

   **Note:**
   *The Attachment size criteria is applied to the total size of each attachment.*

For example, if a message contained two attachments, one a 3 MB attachment and the other a 1 MB attachment, a rule that deletes attachments over 2 MB would delete only the 3 MB attachment. The other attachment would not be deleted.

5.2.3.6.12 Using Attachment Number Criteria

The Attachment number is criteria allow you to create rules that take actions on messages based on the number of attachments the message contains.

1. On the Criteria screen, select Advanced to display the advanced criteria.

2. Select the Attachment number is criteria.

3. Select > or <= from the comparison drop-down list.
   - Select > to apply the rule to messages that are sent with more than the specified number of attachments.
   - Select <= to apply the rule to messages that have the same number or fewer than the specified number of attachments.

   For example:

   >10 apply the rule to all messages that have more than 10 recipients.

   <= 10 apply the rule to all messages that have 10 or fewer recipients.

4. Type the number of attachments to evaluate.

5.2.3.6.13 Using Attachment is Password Protected Criteria

Hosted Email Security can scan the message for a zipped, signed, or password-protected attachment.

1. On the Criteria screen, select Advanced to display the advanced criteria.
2. Select "Any Match".
The Attachment is "password protected" and Recipient number criteria become available.

3. Select Attachment is "password protected".

5.2.3.6.14 Using the Number of Recipients Criteria

The Recipient Number criteria allows you to create rules that take actions on messages based on the number of recipients the message is addressed to.

1. On the Criteria screen, select Advanced to display the advanced criteria.

2. Select "Any Match".
The Attachment is "password protected" and Recipient number criteria become available.

3. Select Recipient number.

4. Select > or <= from the comparison drop-down list.
   - Select > to apply the rule to messages that are sent to more than the specified number of recipients.
   - Select <= to apply the rule to messages that have the same number or fewer than the specified number of recipients.

For example:

   > 10 apply the rule to all messages that have more than 10 recipients.
   <= 10 apply the rule to all messages that have 10 or fewer recipients.

5. Type a value for the number of recipients.

5.2.4 About Rule Actions

Rule actions allow you to specify what happens to messages that satisfy the conditions of the rule's criteria.

Actions fall into these classes:

- "Intercept" actions: Actions in this class intercept the message, preventing it from reaching the original recipient. Intercept actions include deleting the entire message and re-addressing the message.

- "Modify" actions: Actions in this class change the message or its attachments. Modify actions include cleaning cleanable viruses, deleting message attachments, inserting a stamp in the message body, or tagging the subject line.

- "Monitor" actions: Actions in this class allow administrators to monitor messaging. Monitor actions include sending a notification message to others or sending a BCC (blind carbon copy) of the message to others.

- "Scan Limitation" actions: Actions in this class allow administrators to reject or bypass scanning messages that exceed Hosted Email Security capabilities.
"Encrypt Email Message" actions: Actions in this class encrypt the message and then queue it for delivery. This is a non-intercept action, but no other actions can be taken on the target message after this rule is triggered. This action has the lowest priority of all actions, but when triggered it is always the final rule run before the message is queued for delivery. If more than one rule in the rule set is triggered, the rule that uses the encrypt email action will always be triggered last.

**Note:**
This action only applies to outbound rules.

Each rule can contain:

- One and only one intercept action, and
- Any combination of modify or monitor actions

### 5.2.4.1 Specifying Rule Actions

- To add actions to a rule definition, select the desired action.
- To specify details of an action (where required), select the drop-down list, text field, or link that provides more detail for the rule.

For example, if the quarantine action is desired, you need to select which quarantine to send messages to when they trigger this rule. You also might want to create a new quarantine based on an existing one. You can click Edit there to begin that process.

### 5.2.4.2 "Intercept" Actions

"Intercept" actions prevent a message from being delivered to the mailbox of the original recipient. Instead, the message is deleted, quarantined, or sent to a different recipient.

"Intercept" actions are "terminal" actions. Once a terminal action executes, processing of that rule stops and no further action takes place for that rule.

Terminal actions execute following a strict priority order:

1. Delete the entire message.
2. Deliver the message now.
   
   **Warning:**
The Deliver now action is not recommended for use as the only action. If you choose Deliver now as the only action for Spam mail, for example, all of that mail will simply be delivered to your recipients, as if there were no spam filter in place.

   If you use Deliver now with a virus rule, ensure that you also have a Delete action for the virus rule. Only the Delete action takes higher priority than Deliver now and so would be processed before it (and then terminates the processing of that rule).

   If you chose Deliver now as the only action for a virus rule, mail containing viruses would leak through unblocked.
3. Quarantine the message.
4. Re-address to another email recipient.

5.2.4.2.1 Using the Delete Action

This action deletes the message and all attachments. The message is recorded as deleted in the Hosted Email Security logs, but once deleted, the message cannot be recovered. It is one of the "intercept" category of actions. To configure a rule action to delete a message:

Select the Delete entire message action from the "Intercept" section.

5.2.4.2.2 Using the Deliver Now Action

Use the Deliver Now action to deliver email immediately. When this action takes effect, Hosted Email Security delivers the email without executing any more rules for the affected email.

All rules are auto-ordered for security and execution efficiency. Administrators are relieved of determining the order of rule execution. The Deliver Now action bypasses the automatic order of execution so that Hosted Email Security can deliver the email immediately.

Warning:
The Deliver now action is not recommended for use as the only action. If you choose Deliver now as the only action for Spam mail, for example, all of that mail will simply be delivered to your recipients, as if there were no spam filter in place.

If you use Deliver now with a virus rule, ensure that you also have a Delete action for the virus rule. Only the Delete action takes higher priority than Deliver now and so would be processed before it (and then terminates the processing of that rule).

If you chose Deliver now as the only action for a virus rule, mail containing viruses would leak through unblocked.

1. Select the Deliver Now action from the "Intercept" section.
2. Click Next if you are creating a new rule, or Save if you are editing an existing rule.
3. Click OK on the Deliver now warning message that appears. The message closes.
4. If creating a new rule, type a name for the rule in the Rule Name field.

5.2.4.2.3 Using the Change Recipient Action

The Change Recipient action intercepts messages and sends them to a new recipient. This means that the original message recipient will not receive a copy of the message. It is one of the "intercept" class of actions. You can only select a recipient address that is in your domain.

Note:
The Change Recipient action changes the recipient address in the message header. The message will be routed to the new address and the original recipient will not receive the message. The new recipient, however, will see the original recipient’s address in the message header. To have a copy of the message sent to a different address while allowing the original message to go to the original recipient, select the BCC action.
Warning: Redirected messages may contain viruses or malicious code. Trend Micro recommends against redirecting messages to external addresses unless you have configured an outbound virus policy.

1. From the "Intercept" section of the Action page, select the Change Recipient action.

2. Type the email address of the recipient in the field. If you have more than one email address, enter them in the field separated by commas or semicolons.

5.2.4.2.4 Using the Quarantine Action

Quarantined items are now stored in a directory structure created by Hosted Email Security. This structure allows for increased performance when the service is saving items into quarantines or when users view them through the End User Quarantine website. Quarantined messages are indexed in the Hosted Email Security database to provide you with queries and improved search tools.

1. In the "Intercept" section of the Rule Action screen, select the Quarantine action.

2. Select a quarantine area from the drop-down list, or click Edit to create a new quarantine area.

5.2.4.3 "Modify" Actions

"Modify" actions change the message or its attachments. The original sender will still receive the modified message, assuming that the message does not trigger other rules with "Intercept" actions.

5.2.4.3.1 Cleaning Cleanable Viruses

This action will clean cleanable viruses (or other configured threats) contained in message attachments. If the threat cannot be cleaned, the message attachment that contains it will be deleted. Clean cleanable Viruses is one of the "Modify" class of actions.

Important: The Clean cleanable viruses, delete those that cannot be cleaned action is only available in policies with the target criteria of Message contains "viruses or malicious code". If the Clean cleanable viruses, delete those that cannot be cleaned action is used in the rule, and a message contains an uncleanable virus, the attachment will be deleted.

The Delete matching attachments and Clean cleanable viruses, delete those that cannot be cleaned actions cannot be used in the same rule.

To configure a rule action to clean virus-infected attachments:

From the "Modify" section of the Action page, select the Clean cleanable viruses, delete those that cannot be cleaned action.

5.2.4.3.2 Deleting Matching Attachments

This action deletes any attachments that match the rule criteria. It is one of the "Modify" category of actions.

Important: The Delete matching attachments and Clean cleanable viruses, delete those that cannot be cleaned actions cannot be used in the same rule.
The Delete matching attachments action is invoked only when one or more of the following criteria trigger a rule:

- Message contains "viruses or malicious code"
- Attachment is "name or extension"
- Attachment is "MIME content-type"
- Attachment is "true file type"
- Attachment is "password protected"
- Attachment size is
- Attachment content matches "keyword expressions"

For example, a "spam" rule with an action of Delete matching attachments does not delete any attachments if the only target criteria is Message contains "Spam". Add criteria from the list above to use the Delete matching attachments action.

To configure a rule action to delete attachments that match a criteria:

Select Delete matching attachments from the "Modify" section.

5.2.4.3.3 Tagging the Subject Line

The Tag Subject action inserts configurable text into the message subject line. It is one of the "Modify" class of actions.

1. Select the Tag Subject action.
2. Click the tag link. The Tag Subject screen appears.
3. Type a tag in the Tag field.
4. Optionally select Do not tag digitally signed messages.

Note:
Hosted Email Security recognizes messages signed using the S/MIME standard.

5.2.4.3.4 Inserting a Stamp

The Insert stamp in body action inserts a block of text into the message body. The stamps are maintained as named objects in the database and are selected from a list. The stamp definitions contain the text of the stamp (which can contain Hosted Email Security tokens/variables), whether they are to be inserted at the beginning or the end of the message body, and whether or not to avoid stamping TNEF and digitally signed messages to prevent breakage.

Hosted Email Security recognizes messages signed using the S/MIME standard.
1. Select Insert stamp in body.

2. Select from the drop-down list of available stamps.

3. To configure stamps in the list, click Edit.
   See Configuring Stamps.

5.2.4.3.4.4 Configuring Stamps

You can edit or add a new message stamp. Stamps are inserted into messages when they trigger the rule. Typically they contain some standard confidentiality statement or a similar block of text. Rule Tokens/Variables (for example, the name of an attached file) can also be included in the text.

To edit or add a new message stamp:

1. On the Actions page, select Insert stamp in body.

2. Click Edit. The Stamps screen appears, showing a list of available stamps.

3. Click Add or select a stamp from the list and click Edit. The Stamps screen appears, showing details for the stamp.

4. Type a name in the Name field, or edit the existing name if desired.

5. Select whether to insert the stamp at the end or the beginning of the message body.

6. Type the desired text into the text box. Optionally, use rule tokens/variables (such as the an attachment name) as part of the text message.
   See Rule Tokens/Variables.

7. To exclude TNEF and digitally signed messages from stamping, select Do not stamp TNEF and digitally signed messages; prevent breakage.

Note:
Hosted Email Security recognizes messages signed using the S/MIME standard.

The Microsoft TNEF format is used when sending rich text email using the Outlook client. If Hosted Email Security tries to insert a stamp into a TNEF-formatted email, the message might become corrupted or unreadable. To prevent this, if your organization uses Outlook to send rich text formatted messages, Hosted Email Security enables you to exempt TNEF messages from those actions that might corrupt the message.

5.2.4.3.5 Rule Tokens/Variables

Use the following tokens to include variables in message tags and stamps:

<table>
<thead>
<tr>
<th>Token</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SENDER%</td>
<td>Message sender</td>
</tr>
<tr>
<td>%RCPTS%</td>
<td>Message recipients</td>
</tr>
</tbody>
</table>
Table 1. Tokens and Variables

<table>
<thead>
<tr>
<th>Token</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SUBJECT%</td>
<td>Message subject</td>
</tr>
<tr>
<td>%DATE&amp;TIME%</td>
<td>Date and time of incident</td>
</tr>
<tr>
<td>%MAILID%</td>
<td>Mail ID</td>
</tr>
<tr>
<td>%RULENAME%</td>
<td>Name of the rule that contained the triggered filter</td>
</tr>
<tr>
<td>%RULETYPE%</td>
<td>The type of rule: Content Filter, Message Size Filter, and others</td>
</tr>
<tr>
<td>%DETECTED%</td>
<td>Current filter scan result in other task</td>
</tr>
<tr>
<td>%FILENAME%</td>
<td>Name(s) of file(s) that were affected by the rule</td>
</tr>
<tr>
<td>%DEF_CHARSET%</td>
<td>Default character set of the notification message</td>
</tr>
<tr>
<td>%MSG_SIZE%</td>
<td>Total size of the message and all attachments</td>
</tr>
<tr>
<td>%ATTACH_SIZE%</td>
<td>Total size of the attachment(s) that triggered the rule</td>
</tr>
<tr>
<td>%ATTACH_COUNT%</td>
<td>Number of attachments that triggered the rule</td>
</tr>
<tr>
<td>%TACTION%</td>
<td>Terminal action taken by Hosted Email Security</td>
</tr>
<tr>
<td>%ACTION%</td>
<td>All other (non-terminal) actions taken by Hosted Email Security</td>
</tr>
<tr>
<td>%VIRUSNAME%</td>
<td>Name of any virus detected</td>
</tr>
<tr>
<td></td>
<td>This token will be empty if the message did not trigger a virus action.</td>
</tr>
<tr>
<td>%VIRUSACTION%</td>
<td>Action taken on any viruses detected in the message</td>
</tr>
<tr>
<td></td>
<td>This token will be empty if the message did not trigger a virus action.</td>
</tr>
</tbody>
</table>

5.2.4.4 "Monitor" Actions

"Monitor" actions do not change the original message or its attachments. The original sender will still receive the message, assuming that the message does not trigger other rules with intercept actions.

There are two "Monitor" actions:

- Send Notification action
- BCC action

You can combine the first action with any other kind of action. You can combine the BCC action with "modify" actions (and with the first "monitor" action). However, the BCC action cannot be combined with terminal "intercept" actions.

**Tip:**
The notification email message sent to "monitor" actions can be customized using the variables shown in Rule Tokens/Variables.

5.2.4.4.1 About the Send Notification Action
Notifications are messages that are sent when the rule is triggered. They are one of the "Monitor" actions.

You can only send notification messages from addresses within your own domain.

5.2.4.4.1.5 Configuring Send Notification Actions

1. Select a message from the list of those available on the left side of the screen.

2. Click the right arrow button (Add>).
   The selected message appears in the Selected list on the right side.

5.2.4.4.1.6 Deleting Notifications from Rule Actions

1. Select the message you want to delete from the Selected list on the right side.

2. Click Delete.

5.2.4.4.1.7 Deleting Notifications from Lists of Messages

To delete an existing notification message from the list of messages:

1. Select the message you want to delete from the list of those available on the left side of the screen.

2. Click Delete.

5.2.4.4.2 Using the Bcc Action

The BCC action sends a Bcc (blind carbon copy) to a recipient or recipients configured in the rule. It is one of the "monitor" class of actions. You can only configure a notification to be sent to an address in your own domain.

1. From the Monitor section of the Action page, select BCC.

2. Type the email address of the recipient in the field. If you have more than one email address, enter them in the field separated by commas or semicolons.

5.2.4.5 "Scan Limitations" Actions

"Scan limitations" actions can only be used with policies that protect against viruses or malware. They can be combined with any terminal or "Modify" actions.

These are the scan limitation triggers:

- Office 2007/2010 file contains more than 353 files.
- Compressed archive contains more than 353 files.
- Office 2007/2010 file contains a file with decompression ratio of more than 100.
- Compressed file contains a file with decompression ratio of more than 100.
5.2.4.5.1 Rejecting Messages

The Reject the message action deletes the message and sends a Non-Delivery Report (NDR) to the sender. Hosted Email Security message logs record that the message was deleted. Once deleted, the message cannot be recovered.

**Note:**
The Reject the message action is only available in policies with the target criteria of Message contains "viruses or malicious code".

Select the Reject the message action from the "Scan Limitations" section.

5.2.4.5.2 Bypassing Messages

Bypass this rule skips taking any action on the specified message but continues to check the message against the remaining rules in the policy.

**Note:**
The Bypass this rule action is only available in policies with the target criteria of Message contains "viruses or malicious code".

Select the Bypass this rule action from the "Scan Limitations" section.

**Warning:**
The delivered message may contain a security risk.

5.2.4.6 Encrypting Outbound Messages

The purpose of this rule action is to protect sensitive data in email messages sent by users in your organization.

**Note:**
This action only applies to outbound rules.

Actions in this class encrypt the message and then queue it for delivery. This is a non-intercept action, but no other actions can be taken on the target message after this rule is triggered. This action has the lowest priority of all actions, but when triggered it is always the final rule run before the message is queued for delivery. If more than one rule in the rule set is triggered, the rule that uses the encrypt email action will always be triggered last.

In most cases, a rule to encrypt email will be based on one of the following:

- Specific senders or recipients of the message (for example, a rule that encrypts all email sent from Human Resources or the Legal department)
- Specific content in the message body

1. From the "Intercept" section of the Action page, select Do not intercept messages
2. From the "Modify" section of the page, select the Encrypt email action.

5.2.5 Naming and Enabling a Rule

Once you have created a rule, the final step is to name and enable it. You can also add notes.

1. On the Rule tab:
a. Name the rule.

**Note:**
Trend Micro recommends using a descriptive name that will allow administrators to easily identify this rule from the list in the Policy screen. For instance, if you are creating a spam rule that applies to the one.example.com domain, you might name it something like "One Example Spam Rule".

b. Click Enable to put the rule into effect.

c. Review the rule definition summarized in the box. If anything in any of the three sections needs changing, you can click on the links to return to that step of the rule definition and make the change.

2. On the Notes tab, enter any notes about this rule.

3. Click Save.

   The Policy screen is displayed, with your rule in the appropriate order and highlighted in the list.

**5.3 Configuring Sender Filter**

Configure the Approved Senders and Blocked Senders lists to control which email messages Hosted Email Security scans. Specify the senders to allow or block using specific email addresses or entire domains.

For example, *@example.com specifies all senders from the example.com domain.

Evaluation is done in the following order:

1. End User Quarantine website Approved Senders lists
2. Administrator console Approved Senders lists
3. End User Quarantine website Blocked Senders lists
4. Administrator console Blocked Senders lists

See [Sender Filter Order of Evaluation](#).

**Tip:**

*IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.*

See [General Order of Evaluation](#).

Lists of approved or blocked senders are managed using the following screens:

- Approved Senders

  Email messages from senders added to this list are not subject to IP reputation-based, spam, phish, or marketing message filtering. Hosted Email Security still performs malware and attachment scanning on all messages received and takes the action configured in policy rules after detecting a malware threat or an attachment policy violation.
Go to Sender Filter > Approved Senders to display this screen.

- **Blocked Senders**

Hosted Email Security automatically blocks messages sent from addresses or domains added to the blocked list without subjecting the messages to any scanning.

Go to Sender Filter > Blocked Senders to display this screen.

The Approved Senders and Blocked Senders tables display the following information:

- **Sender**: The email address or domain that you approved or blocked for the specified Recipient Domain
- **Recipient Domain**: The managed domain for which you approved or blocked the specified sender
- **Date Added**: The date that you added the sender to the list

### 5.3.1 Adding Senders

Hosted Email Security only approves or blocks email messages from the specified sender for the specified domain.

For example, after adding spammerbob@examplespamdomain.com to the blocked list for your managed domain mydomain.com, Hosted Email Security only blocks the email messages sent from spammerbob@examplespamdomain.com to addresses in the mydomain.com domain. Hosted Email Security still scans and possibly passes email messages sent from spammerbob@examplespamdomain.com to your other managed domains.

To block or allow email messages from a specific sender to all domains, select all my domains from the Managed domain drop-down list.

1. Select a specific domain from the Managed domain drop-down list. To select all domains, select all my domains from the list.
   
   ![Managed domain list](image)

2. In the Email address or domain field, type a sender. A sender can be a specific email address or all addresses from a specific domain or subdomain.
   
   - Filter a specific email address by typing that email address.
   
   - Filter 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 filter all email addresses in the example.com domain.

   - Filter all addresses from a subdomain by using an asterisk (*) to the left of the at sign (@) and also using an asterisk (*) in place of the subdomain in the email address. For example, *@*.example.com will filter all email addresses in all subdomains of the example.com domain.

The following table displays format examples that are valid or not valid:

<table>
<thead>
<tr>
<th>Valid Email Address</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>*@example.com</td>
<td>Yes</td>
</tr>
<tr>
<td>*@example.com@com</td>
<td>Yes</td>
</tr>
<tr>
<td><em>@</em>.example.com</td>
<td>Yes</td>
</tr>
<tr>
<td>*@example.com example.com</td>
<td>No</td>
</tr>
</tbody>
</table>

**Table 1. Format Examples for Approved Senders and Blocked Senders**
3. Click Add to List Hosted Email Security validates the sender address and adds it to the list.

Tip:
Hosted Email Security validates the format of the sender address before adding the sender to the list. If you receive multiple formatting errors messages and are sure that the address provided is accurate, your administrator console may have timed out. Reload the page and try again.

5.3.2 Editing Senders

1. Select a specific domain from the Managed domain drop-down list. To select all domains, select all my domains from the list.

2. Click the email address or domain of a sender. The email address or domain becomes editable, and buttons labeled OK or Cancel appear.

3. Make and confirm your changes or corrections.
   • Filter a specific email address by typing that email address.
   • Filter 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 filter all email addresses in the example.com domain.
   • Filter all addresses from a subdomain by using an asterisk (*) in place of the subdomain in the email address. For example, *@*.example.com will filter all email addresses in all subdomains of the example.com domain.

The following table displays format examples that are valid or not valid:

<table>
<thead>
<tr>
<th>Valid</th>
<th>Not Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:name@info.example.com">name@info.example.com</a></td>
<td>name@*.example.com</td>
</tr>
<tr>
<td>*@example.com</td>
<td><em>@</em>.com</td>
</tr>
<tr>
<td>*@server.example.com</td>
<td><em>@</em></td>
</tr>
<tr>
<td><em>@</em>.example.com</td>
<td></td>
</tr>
</tbody>
</table>
5.4 Understanding IP Reputation

Hosted Email Security offers two tiers of protection. IP reputation-based filtering at the MTA connection level, provided by Trend Micro Email Reputation Services (ERS), is the first tier. The second is content-based filtering at the message level.

**Tip:**

IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.

See [IP Reputation-Based Filtering at the MTA Connection Level](#).
See [General Order of Evaluation](#).
See [IP Reputation Order of Evaluation](#).

Hosted Email Security makes use of Trend Micro Email Reputation Services (ERS) Standard Service and Advanced Service. Email Reputation Services uses a standard IP reputation database and an advanced, dynamic IP reputation database (a database updated in real time). These databases have distinct entries, allowing Trend Micro to maintain a very efficient and effective system that can quickly respond to new sources of spam.

Configure the following settings on the IP Reputation Settings screen:

- Dynamic Reputation Settings control how Hosted Email Security uses the dynamic IP reputation database from Email Reputation Services Advanced Service.
- Standard IP Reputation Settings control how Hosted Email Security uses the standard IP reputation database from Email Reputation Services Standard Service.

The Approved and Blocked IP Addresses screen shows approved and blocked countries, Internet service providers, IP addresses, and CIDR blocks.

### 5.4.1 About Dynamic IP Reputation Settings

Hosted Email Security makes use of Trend Micro Email Reputation Services (ERS) Standard Service and Advanced Service.

Dynamic IP Reputation Settings use Trend Micro Email Reputation Services Advanced Service, a real-time anti-spam solution. The Trend Micro network of automated expert systems, along with Trend Micro spam experts, continuously monitor network and traffic patterns and immediately update the dynamic IP reputation database as new spam sources emerge, often within minutes. As evidence of spam activity increases or decreases, the dynamic IP reputation database is updated accordingly.

The dynamic IP reputation database includes the following blocking levels:

- **Level 0: Off**
  Queries the dynamic reputation database but does not block any IP addresses.

- **Level 1: Least aggressive**
  Hosted Email Security allows the same amount of spam from a sender with a good rating as in Level 2. The length of time that the IP address stays in the database is generally shorter than for more aggressive settings.
• Level 2: (the default setting)

Hosted Email Security allows a larger volume of spam from a sender with a good rating than more aggressive settings. However, if an increase in spam above the allowable threshold is detected, it adds the sender to the dynamic reputation database. The length of time that the IP address stays in the database is generally shorter than for more aggressive settings.

• Level 3:

Hosted Email Security allows a small volume of spam from senders with a good rating. However, if an increase in spam beyond the allowable threshold is detected, it adds the sender to the dynamic reputation database. The length of time that the IP address stays in the database depends on whether additional spam from the sender is detected.

• Level 4: Most aggressive

If even a single spam message from a sender IP address is detected, Email Reputation Services adds the sender to the dynamic reputation database and Hosted Email Security blocks all messages from the sender. The length of time that the IP address stays in the database depends on whether additional spam from the sender is detected.

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

Note:
To avoid false positives from a trusted partner company, go to IP Reputation > Approved/Blocked and add the IP address for their MTA to the Approved list.
The IP addresses in the Approved lists bypass other IP reputation-based filtering. This list is useful for ensuring all messages from a partner company or other MTA are allowed, no matter their status with the standard IP reputation databases or with the Trend Micro Email Reputation Services (ERS) dynamic IP reputation database. When using the IP reputation approved lists, you may experience lower overall spam catch rates.

5.4.2 About Standard IP Reputation Settings

Hosted Email Security makes use of Trend Micro Email Reputation Services (ERS) Standard Service and Advanced Service.

See IP Reputation-Based Filtering at the MTA Connection Level.

Standard IP Reputation Settings use Trend Micro Email Reputation Services Standard Service, which helps block spam by validating requested IP addresses against the Trend Micro standard IP reputation database, powered by the Trend Micro Threat Prevention Network. This ever-expanding database currently contains over a billion IP addresses with reputation ratings based on spamming activity. Trend Micro spam investigators continuously review and update these ratings to ensure accuracy.

Hosted Email Security makes a query to the standard IP reputation database server whenever it receives an email message from an unknown host. If the host is listed in the standard IP reputation database, that message is reported as spam.
You can choose which lists to enable from the standard IP reputation database. By default, all lists are enabled. The default setting is the most effective for reducing spam levels, and it meets the needs of most customers.

**Note:**
*If you disable some portions of the standard IP reputation database, you may see an increase in the amount of spam messages that reach your internal mail server for additional content filtering.*

The standard IP reputation database includes the following lists:

- **Known Spam Source:** The Real-time Blackhole List (RBL) is a list of IP addresses of mail servers that are known to be sources of spam.

- **Dynamically Assigned IP:** The Dynamic User List (DUL) is a list of dynamically assigned IP addresses, or those with an acceptable use policy that prohibits public mail servers. Most entries are maintained in cooperation with the ISP owning the network space. IP addresses in this list should not be sending email directly but should be using the mail servers of their ISP.

**Note:**
*To avoid false positives from a trusted partner company, go to IP Reputation > Approved/Blocked and add the IP address for their MTA to the Approved list.*

**The IP addresses in the Approved lists bypass other IP reputation-based filtering. This list is useful for ensuring all messages from a partner company or other MTA are allowed, no matter their status with the standard IP reputation databases or with the Trend Micro Email Reputation Services (ERS) dynamic IP reputation database. When using the IP reputation approved lists, you may experience lower overall spam catch rates.**

### 5.4.3 About Approved and Blocked IP Addresses

Go to IP Reputation > Approved/Blocked to display this screen.

To manually override IP reputation-based filtering at the MTA connection level, add IP addresses to the lists on the Approved and Blocked IP Addresses screen. These lists override the Dynamic IP Reputation Settings and Standard IP Reputation Settings and allow for customization of which addresses are subjected to IP reputation-based filtering.

There are lists of approved and blocked countries, IP addresses, and Classless Inter-Domain Routing (CIDR) blocks.

**Tip:**
*To add a CIDR block to the list, type the IPv4 address / CIDR block. The following is the only valid format: x.x.x.x/z*

The IP addresses in the Approved lists bypass other IP reputation-based filtering. This list is useful for ensuring all messages from a partner company or other MTA are allowed, no matter their status with the standard IP reputation databases or with the Trend Micro Email Reputation Services (ERS) dynamic IP reputation database. When using the IP reputation approved lists, you may experience lower overall spam catch rates.

The IP addresses in the Blocked lists are not subject to other IP reputation-based filtering. Hosted Email Security permanently rejects connection attempts from such IP addresses by responding with a 550 error (a rejection of the requested connection).
**Tip:**
IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.

See *Configuring Sender Filter*.

### 5.4.4 Troubleshooting Issues

If you encounter unexpected errors while trying to save your settings on the IP Reputation Settings screen, you may be able to resolve the issue on your own. Consult the following table for guidance on resolving the problem before contacting technical support.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Possible Cause</th>
<th>Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Save button is disabled.</td>
<td>You do not have a valid Activation Code.</td>
<td>Obtain a valid Activation Code from your vendor.</td>
</tr>
<tr>
<td></td>
<td>You have applied for an Activation Code, but it has not yet been added to the Hosted Email Security system.</td>
<td>Try again later.</td>
</tr>
<tr>
<td></td>
<td>A temporary network issue is preventing Hosted Email Security from validating the Activation Code.</td>
<td>Try again later.</td>
</tr>
<tr>
<td>I cannot save my IP Reputation settings.</td>
<td>There is a temporary network issue.</td>
<td>Try again later.</td>
</tr>
<tr>
<td></td>
<td>There is more than one browser window open to the Hosted Email Security administrator console, and the session in one of the other windows has expired.</td>
<td>Close the other windows and try again.</td>
</tr>
</tbody>
</table>

### 5.5 Understanding Advanced Protection

Hosted Email Security advanced protection allows you to better secure data and ensure communication privacy for email traffic in your Managed Domains.

#### 5.5.1 About Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol that helps to secure data and ensure communication privacy between endpoints. Hosted Email Security allows you to configure TLS encryption policies between Hosted Email Security and specified TLS peers. Hosted Email Security supports the following TLS protocols in descending order of priority: TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0.

The Transport Layer Security (TLS) screen uses the following important terms:
<table>
<thead>
<tr>
<th>Term</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS peer</td>
<td>Hosted Email Security can apply your specified TLS configuration with this domain during network communications.</td>
</tr>
</tbody>
</table>
| Security level     | **Opportunistic:**  
• Communicates using encryption if the peer supports and elects to use TLS  
• Communicates without encryption if the peer does not support TLS  
• Communicates without encryption if the peer supports TLS but elects not to use TLS  

**Mandatory:**  
• Communicates using encryption if the peer supports and elects to use TLS  
• Does not communicate if the peer does not support TLS  
• Does not communicate if the peer supports TLS but elects not to use TLS  

**Important:**  
Because of the risk of losing data, Trend Micro recommends confirming TLS encrypted message delivery between a Managed Domain and a peer before using the Mandatory security level.  

See Testing TLS.  

To ensure messages can be received from the Hosted Email Security MTA, configure your firewall to accept email messages from the following Hosted Email Security IP address / CIDR blocks:  

• 216.104.0.0/24  
• 216.99.128.0/24  
• 150.70.0.0/24 – All Regions  
• 54.219.191.0/25 – North and South America, Asia, and Japan Regions  
• 54.86.63.64/26 – North and South America, Asia, and Japan Regions  
• 52.58.63.0/25 – Europe, Middle-east and Africa (EMEA) Regions  
• 52.58.62.192/26 – Europe, Middle-east and Africa (EMEA) Regions  
• 52.48.127.192/26 – Europe, Middle-east and Africa (EMEA) Regions  

| Status             | • Enabled: Hosted Email Security applies your specified TLS configuration to the peer  
• Disabled: Hosted Email Security does not apply your specified TLS configuration to the peer  

Instead, the "Default" TLS configuration applies.                                                                                                                                                                                                 |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default (TLS Peer) | This configuration applies to all domains that meet any of the following criteria:  
• Domain is not in the peer list  
• Domain is in the peer list, but is not enabled                                                                                                                                                                                                 |

### 5.5.1.1 Testing TLS

**Important:**  
Because of the risk of losing data, Trend Micro strongly recommends doing the following before specifying a Security Level of Mandatory:  

• Confirm TLS encrypted message delivery between Hosted Email Security and your Managed Domain.
• Confirm the TLS configuration for any peers on the Internet. Contact the managers of each peer yourself. Trend Micro is unable to assist you in this process.

Use the following procedure to test TLS between Hosted Email Security and the email server for your Managed Domain.


2. Select a Managed Domain.

3. Select the Direction of Incoming. Test TLS appears at the top-right of the screen.

4. Click Test TLS.

5. Specify the Send test message to email address.

6. Click Send Test. Hosted Email Security sends a message to the specified email address confirming TLS works for the Managed Domain.

**Tip:** If the message does not arrive within a short period of time, confirm that the email server for the Managed Domain is correctly configured to use TLS. After verifying the server configuration, send the test again.

### 5.5.1.2 Adding TLS Peers


2. Select a Managed Domain.

3. Select the Direction of Incoming or Outgoing.

4. Specify the TLS Peer to add.

5. Set the Security level to one of the following:
   - Opportunistic:
     - Communicates using encryption if the peer supports and elects to use TLS
     - Communicates without encryption if the peer does not support TLS
     - Communicates without encryption if the peer supports TLS but elects not to use TLS
   
   - Mandatory:
     - Communicates using encryption if the peer supports and elects to use TLS
     - Does not communicate if the peer does not support TLS
     - Does not communicate if the peer supports TLS but elects not to use TLS
Important:
Because of the risk of losing data, Trend Micro recommends confirming TLS encrypted message delivery between a Managed Domain and a peer before using the Mandatory security level.

See Testing TLS.

To ensure messages can be received from the Hosted Email Security MTA, configure your firewall to accept email messages from the following Hosted Email Security IP address / CIDR blocks:
HES IP addresses

6. Select Enabled to have Hosted Email Security apply your specified TLS security level to the new peer.

7. Click Add.

5.5.1.3 Editing TLS Peers


2. Select a Managed Domain.

3. Select the Direction of Incoming or Outgoing.

4. To the right of a peer in the list, click Edit.

5. Reconfigure the peer.

6. Click Save.

5.5.2 About Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is an open standard to prevent sender address forgery. The SPF protects the envelope sender address, which is used for the delivery of messages. Hosted Email Security enables you to configure SPF to ensure sender's authenticity.

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

Evaluation of an SPF record can return any of the following results:

<table>
<thead>
<tr>
<th>Result</th>
<th>Explanation</th>
<th>Intended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>The SPF record designates the host to be allowed to send.</td>
<td>Accept</td>
</tr>
<tr>
<td>Fail</td>
<td>The SPF record has designated the host as NOT being allowed to send.</td>
<td>Reject</td>
</tr>
<tr>
<td>Result</td>
<td>Explanation</td>
<td>Intended Action</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SoftFail</td>
<td>The SPF record has designated the host as NOT being allowed to send but is in transition.</td>
<td>Accept</td>
</tr>
<tr>
<td>Neutral</td>
<td>The SPF record specifies explicitly that nothing can be said about validity.</td>
<td>Accept</td>
</tr>
<tr>
<td>None</td>
<td>The domain does not have an SPF record or the SPF record does not evaluate to a result.</td>
<td>Accept</td>
</tr>
<tr>
<td>PermError</td>
<td>A permanent error has occurred (for example, badly formatted SPF record).</td>
<td>Accept</td>
</tr>
<tr>
<td>TempError</td>
<td>A transient error has occurred.</td>
<td>Accept</td>
</tr>
</tbody>
</table>

### 5.5.2.1 Enabling or Disabling Sender Policy Framework (SPF)

You can enable Sender Policy Framework (SPF) to allow Hosted Email Security to evaluate the legitimacy of sender's email address, before delivering the email to the recipient.

1. Go to Advanced Protection > Sender Policy Framework (SPF).

2. Select Enable Sender Policy Framework to enable SPF in Hosted Email Security. Clear this check-box to disable SPF.

3. Click OK on the confirmation dialog box.

   **Note:** The confirmation dialog box only appears if the domain selected in Managed Domain is all my domains.

4. If you also want to add the SPF check result into the email message's xheader, select Add SPF DNS check result into message's xheader, and then click OK on the confirmation dialog box. Clear this check-box to disable this setting. Hosted Email Security adds messages similar to the following in email message's xheader named X-TM-Received-SPF:

<table>
<thead>
<tr>
<th>Status</th>
<th>X-TM-Received-SPF: Pass (domain of <a href="mailto:example_address@example.com">example_address@example.com</a> designates 10.64.72.206 as permitted sender) client-ip=10.64.72.206; envelope-from=<a href="mailto:example_address@example.com">example_address@example.com</a>; helo=imsva-1382.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail</td>
<td>X-TM-Received-SPF: Fail (domain of <a href="mailto:example_address@example.com">example_address@example.com</a> does not designates 10.64.72.206 as permitted sender) client-ip=10.64.72.206; envelope-from=<a href="mailto:example_address@example.com">example_address@example.com</a>; helo=imsva-1382.com</td>
</tr>
<tr>
<td>SoftFail</td>
<td>X-TM-Received-SPF: SoftFail (domain of transitioning <a href="mailto:example_address@example.com">example_address@example.com</a> discourages use of 10.64.72.206 as permitted sender) client-ip=10.64.72.206; envelope-from=<a href="mailto:example_address@example.com">example_address@example.com</a>; helo=imsva-1382.com</td>
</tr>
</tbody>
</table>
### 5.5.2.2 Adding an SPF Peer to the Ignored List

Hosted Email Security enables you to add SPF peers to the ignored list. If SPF is enabled, Hosted Email Security ignores the SPF peers that are included in this list, and does not perform verification for these peers.

1. Go to Advanced Protection > Sender Policy Framework (SPF).
2. In Ignored Peer field, type a sender domain name, IP address or IP/CIDR block that you want to ignore for verification.
3. Click Add to List.

### 5.5.2.3 Editing an SPF Peer in the Ignored List

1. Go to Advanced Protection > Sender Policy Framework (SPF).
2. From the list of SPF Peers, click Edit before the peer whose domain name, IP address or IP/CIDR block you want to modify.
3. Modify the information in the field displayed, and then click Save.

### 5.5.2.4 Deleting SPF Peers from Ignored List

1. Go to Advanced Protection > Sender Policy Framework (SPF).
2. From the list of SPF peers, select the peers that you want to delete, and then click Delete.
3. Click OK on the confirmation dialog box.

5.6 Understanding Quarantine

Quarantined messages are blocked as detected spam or other inappropriate content before delivery to an email account. Messages held in quarantine can be reviewed and manually deleted or delivered.

**Warning:**
*Hosted Email Security automatically deletes messages from the quarantine after 30 days.*

To manage messages for other members of a managed domain, the Query screen of the administrator console must be used.

Quarantine management in the administrator console is divided into the following parts:

- Use the Quarantine > Query screen to view a list of quarantined messages for your managed domains. You can review messages, delete them, or release them for further filtering.

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

- Use the Digest Settings screen to configure the schedule and format for the Quarantine Digest. If the digest is enabled, all domain recipients receive their own customized copy of the digest. Intended message recipients can use the End User Quarantine website to manage messages in quarantine themselves.

  **Note:**
  *To allow intended recipients use the End User Quarantine website to manage messages in quarantine themselves, do the following:*

  - Configure policy rules to quarantine messages:
    See [Managing Policy Rules](#).

  - Share the End User Quarantine User's Guide and the following web address for your region with end users:
    - For Europe, the Middle East, Africa: [https://euq.hes.trendmicro.eu](https://euq.hes.trendmicro.eu)
    - For all other regions: [https://euq.hes.trendmicro.com](https://euq.hes.trendmicro.com)

5.6.1 Querying the Quarantine

Use the Quarantine > Query screen to view a list of quarantined messages for your managed domains. You can review messages, delete them, or release them for further filtering.

1. In the Dates fields, select a range of dates.

  **Note:**
  *Queries include data for up to seven continuous days in one calendar month. Use more than one query to search across calendar months.*
2. In the Direction field, select a mail traffic direction.

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

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

4. The following table displays format examples that are valid or not valid:

   Table 1. Format Examples for Mail Tracking and Quarantine Query

<table>
<thead>
<tr>
<th>Valid</th>
<th>Not Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:name@info.example.com">name@info.example.com</a></td>
<td>name*@.example.com</td>
</tr>
<tr>
<td>*@example.com</td>
<td><em>@</em>.com</td>
</tr>
<tr>
<td>*@server.example.com</td>
<td>@*</td>
</tr>
<tr>
<td>@*.example.com</td>
<td></td>
</tr>
</tbody>
</table>

   4. Click Search.

   5. Select the messages to manage.

   6. Click one of the following buttons to manage selected messages:
   - Delete: Cancel delivery and permanently delete the message
   - Deliver (Not Spam): Release from quarantine

   **Note:**
   Released messages are no longer marked as spam, but they will continue to be processed by Hosted Email Security. The following conditions apply to delivery:
   - 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.
   - 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.
5.6.2 About the Quarantine Digest

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

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

Use the Digest Settings screen to configure the schedule and format for the Quarantine Digest. If the digest is enabled, all domain recipients receive their own customized copy of the digest. Intended message recipients can use the End User Quarantine website to manage messages in quarantine themselves.

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

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

**Warning:**

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

The Quarantine Digest Inline Action feature supports only client computers running Microsoft Windows XP Service Pack 3 or later and using only one of the following email clients:

- Microsoft Outlook 2003 Service Pack 3 or later
- Microsoft Outlook Express 6.0 or later
### Configuring the Quarantine Digest

1. Go to Quarantine > Digest Settings.

2. Enable sending Quarantine Digest email messages (disabled by default) using the button at the top-right of the screen.

   **Tip:**
   *The toggle button shows the current enabled [ ] or disabled [ ] state of the setting. Click the button to switch the state of the setting.*

3. Select a specific domain from the Managed domain drop-down list.

4. In the Frequency drop-down list, select the frequency with which to send the digest:
   - Daily: Specify to send the digest a maximum of three times daily.

   **Tip:**
   *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. Right-click any of the following fields to display a list of available and selectable tokens for the field.*

   - Weekly: Specify the days of the week and time of day to send the digest.

   **Warning:**
   *Hosted Email Security automatically deletes messages from the quarantine after 30 days.*

5. Under Digest Mail Template for `<managed_domain>`, configure the following settings:

   **Tip:**
   *Use the add [ ] and the remove [ ] buttons to manage additional entries.*

   - From: Specify the email address that the digest displays in the From field.

   **Table 1. From Field Digest Tokens**

<table>
<thead>
<tr>
<th>Token</th>
<th>Content in Sent Digest Email Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>%DIGEST_RCPT%</td>
<td>Digest recipient's email address appears in the From field of the received digest email message</td>
</tr>
</tbody>
</table>
• Subject: Specify the subject line for the digest.

Table 2. Subject Field Digest Tokens

<table>
<thead>
<tr>
<th>Token</th>
<th>Content in Sent Digest Email Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>%DIGEST_RCPT%</td>
<td>Digest recipient's email address appears in the subject line</td>
</tr>
<tr>
<td>%DIGEST_DATE%</td>
<td>Digest date appears in the subject line</td>
</tr>
</tbody>
</table>

• HTML content:

  ▪ Specify if Inline Action should be Enabled or Disabled using the toggle button above the HTML content field.

  ▪ Specify the HTML content of the digest if the email client accepts HTML messages.

Table 3. HTML Content Field Digest Tokens

<table>
<thead>
<tr>
<th>Token</th>
<th>Content in Sent Digest Email Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>%DIGEST_RCPT%</td>
<td>Digest recipient's email address appears in HTML body of message</td>
</tr>
<tr>
<td>%DIGEST_DATE%</td>
<td>Digest date appears in HTML body of message</td>
</tr>
<tr>
<td>%DIGEST_BODY_HTML%</td>
<td>Digest summary in HTML table format appears in HTML body of message</td>
</tr>
<tr>
<td>%DIGEST_PAGE_COUNT%</td>
<td>Total number of quarantined messages in listed digest summary (up to 100 maximum) appears in HTML body of digest email message</td>
</tr>
<tr>
<td>%EUQ_HOST_SERVER%</td>
<td>Address of Hosted Email Security End User Quarantine website appears in HTML body of digest email message</td>
</tr>
</tbody>
</table>

• Plain text content: Specify the plain text content of the digest if the email client only accepts plain text messages.

Table 4. Plain Text Content Field Digest Tokens

<table>
<thead>
<tr>
<th>Token</th>
<th>Content in Sent Digest Email Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>%DIGEST_RCPT%</td>
<td>Digest recipient's email address appears in text body of message</td>
</tr>
<tr>
<td>%DIGEST_DATE%</td>
<td>Digest date appears in text body of message</td>
</tr>
<tr>
<td>%DIGEST_BODY_TEXT%</td>
<td>Digest summary in plain text format appears in text body of message</td>
</tr>
<tr>
<td>%DIGEST_PAGE_COUNT%</td>
<td>Total number of quarantined messages listed in the digest summary (up to 100 maximum) appears in plain text body of digest email message</td>
</tr>
<tr>
<td>%EUQ_HOST_SERVER%</td>
<td>Address of Hosted Email Security End User Quarantine website appears in HTML body of digest email message</td>
</tr>
</tbody>
</table>
5.7 Understanding Mail Tracking

This screen is optimized for tracking "missing" messages.

Trend Micro Hosted Email Security maintains up to 30 days of mail tracking information.

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

When you query the mail tracking information, Hosted 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.

The Mail Tracking query results are displayed in tabs:

- **Blocked Traffic:** Attempts to send messages that were stopped by IP reputation-based filtering at the MTA connection level or by Hosted Email Security incoming security filtering.

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

  The display of Blocked Traffic has different meanings for incoming and outgoing traffic. Incoming traffic is filtered by Trend Micro Email Reputation Services and by Hosted Email Security incoming security filtering; outgoing traffic is not. If messages are blocked in outgoing traffic, the reason for blocking is unrelated to email reputation but may be related to Hosted Email Security relay mail service filtering.

- **Accepted Traffic:** Messages that were allowed in by Hosted Email Security for further processing.

- **Unresolved Traffic:** Messages that cannot be uniquely identified by their Sender Message ID because the ID is null.

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:

- Expand the result set by omitting the recipient.

- If the sender is actually blocked by IP reputation-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.

- 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.

- 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.

### 5.7.1 About the Blocked Traffic Tab

This tab displays a summary of matched sender MTA IPs that were either permanently or temporarily blocked by Trend Micro Email Reputation Services and Hosted Email Security incoming security filtering (for incoming messages) or by Hosted Email Security relay mail service filtering (for outgoing messages).

When data is available in the Blocked Traffic tab, it will be displayed by default. Also, an email message may be permanently rejected by Hosted Email Security due to its exceedingly large size, for example, if the size of a message exceeds 50 MB.

The following Blocked Traffic information is displayed:

- **Timestamp:** The time the message attempt was blocked. Click on the Timestamp value to view Mail Tracking Details for a given message.

- **Sender:** The sender email address on the message envelope, in other words, the sender address in the SMTP MAIL command.

- **Recipient:** The first recipient email address on the message envelope, in other words, the recipient in the first SMTP RCPT command.

- **Blocked:**
  - For incoming messages: The sender IP address was blocked by Email Reputation Services or Hosted Email Security content-based filtering at the message level.

    Blocked status is either Temporary or Permanent.

    If the message has an exceedingly large size, the status will display Size limit. In this case, the message is rejected and blocked permanently by Hosted Email Security content-based filtering due to its size. Hosted Email Security will respond to the sending MTA with a 552 error (a failure of the requested connection because the message exceeded storage allocation).

  - For outgoing messages: The message was blocked by Hosted Email Security relay mail service filtering. Outgoing messages are not filtered by Email Reputation Services (ERS). Outgoing messages can be blocked for the following reasons:
    
    o The recipient address is not resolvable, for example someone@???.com.
    
    o Spammers forged the message sender to be in the customer domain.
    
    o Your MTA is compromised, for example it is an open relay, and it is sending spam messages.

- **Sender IP:** The IP address of the upstream MTA that delivered this message to Hosted Email Security.
5.7.2 About the Accepted Traffic Tab

This tab displays a summary of matching messages that were accepted by Trend Micro Hosted Email Security.

When you click on the Accepted Traffic tab, you will see a summary of the matching email message traffic that was accepted by Trend Micro Hosted Email Security. Once a message is accepted, it goes through various stages of processing by Hosted Email Security.

See Content-Based Filtering at the Message Level.

This result summary is organized with recipient in mind, since mail tracking is mostly initiated by an end user. For a message that has multiple recipients, the result will be organized as one recipient per entry.

The following information is displayed for Accepted Traffic:

- **Timestamp**: The time the message was accepted by Hosted Email Security. Click on the Timestamp value to open the Mail Tracking Details window for a given message.
- **Sender**: The sender email address on the message envelope, in other words, the sender address in the SMTP MAIL command.
- **Recipient**: The first recipient email address on the message envelope, in other words, the recipient in the first SMTP RCPT command.
- **Action**: The last action taken on the message. For all the actions, see Actions below.
  - Delivered: The message has been delivered to the downstream MTA that is responsible for transporting the message to its destination.
  - Bounced: The message has been rejected by the downstream MTA. Hosted Email Security will attempt to notify the sender about the event.
  - Deleted: The message has been deleted by Hosted Email Security according to the policy established by the authorized mail administrator of this mail domain.
  - Redirected: The message has been redirected to a different recipient according to the Hosted Email Security policy established by the authorized mail administrator of this mail domain.
  - Expired: Hosted Email Security attempted delivery repeatedly over several days without success and decided that the message is undeliverable. Hosted Email Security will attempt to notify the sender about the event.
  - Queued for delivery: The message is ready to be delivered to the downstream MTA that is responsible for transporting the message to its destination. This is a transient state of this message; it should not remain in this state for an extended period of time.
  - Temporary delivery error: The message should be ready to be delivered to the downstream MTA that is responsible for transporting the message to its destination. However, something is preventing the message from posting. This is a transient state of this message; it should not remain in this state for an extended period of time.
- Quarantined: Quarantined messages are blocked as detected spam or other inappropriate content before delivery to an email account. Messages held in quarantine can be reviewed and manually deleted or delivered.

- Encryption in progress: The message is being encrypted by Hosted Email Security. After encryption is complete, Hosted Email Security will queue the message for delivery.

- Others: All not listed above.

- **Subject:** The subject line (if available) of the message.

- **Sender IP:** The IP address of the upstream MTA that delivered this message to Hosted Email Security.

- **Delivered to:** The IP address of the downstream MTA that accepted delivery of this message. This is only available when the action is "Delivered".

- **Size(KB):** The size of the message. This information is not always available.

### 5.7.3 About the Unresolved Traffic Tab

- The following information is displayed for Unresolved Traffic:

  - **Timestamp:** The time the message was accepted by Hosted Email Security. Click on the Timestamp value to open the Mail Tracking Details window for a given message.

  - **Sender:** The sender email address on the message envelope, in other words, the sender address in the SMTP MAIL command.

  - **Recipient:** The first recipient email address on the message envelope, in other words, the recipient in the first SMTP RCPT command.

  - **Action:** The last action taken on the message. For all the actions, see Actions below.

- **Delivered:** The message has been delivered to the downstream MTA that is responsible for transporting the message to its destination.

- **Bounced:** The message has been rejected by the downstream MTA. Hosted Email Security will attempt to notify the sender about the event.

- **Deleted:** The message has been deleted by Hosted Email Security according to the policy established by the authorized mail administrator of this mail domain.

- **Redirected:** The message has been redirected to a different recipient according to the Hosted Email Security policy established by the authorized mail administrator of this mail domain.

- **Expired:** Hosted Email Security attempted delivery repeatedly over several days without success and decided that the message is undeliverable. Hosted Email Security will attempt to notify the sender about the event.

- **Queued for delivery:** The message is ready to be delivered to the downstream MTA that is responsible for transporting the message to its destination. This is a transient state of this message; it should not remain in this state for an extended period of time.
• Temporary delivery error: The message should be ready to be delivered to the downstream MTA that is responsible for transporting the message to its destination. However, something is preventing the message from posting. This is a transient state of this message; it should not remain in this state for an extended period of time.

• Quarantined: Quarantined messages are blocked as detected spam or other inappropriate content before delivery to an email account. Messages held in quarantine can be reviewed and manually deleted or delivered.

• Encryption in progress: The message is being encrypted by Hosted Email Security. After encryption is complete, Hosted Email Security will queue the message for delivery.

• Others: All not listed above.

• Subject: The subject line (if available) of the message.

• Sender IP: The IP address of the upstream MTA that delivered this message to Hosted Email Security.

• Delivered to: The IP address of the downstream MTA that accepted delivery of this message. This is only available when the action is "Delivered".

• Size(KB): The size of the message. This information is not always available.

• Sender Message ID: A unique identifier for the message. This information is not always available.

5.7.4 Social Engineering Attack Log Details

Hosted Email Security provides detailed information for email messages detected as possible social engineering attacks. To view social engineering attack details, click the Details link beside Social engineering attack on the Mail Tracking Details screen.

The following table lists the possible reasons for social engineering attack detections.

<table>
<thead>
<tr>
<th>Email Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconsistent sender host names</td>
<td>Inconsistent host names between Message-ID (&lt;domain&gt;) and From (&lt;domain&gt;).</td>
</tr>
<tr>
<td>Broken mail routing path</td>
<td>Broken mail routing path from hop (&lt;IP_address&gt;) to hop (&lt;IP_address&gt;).</td>
</tr>
<tr>
<td>Mail routing path contains mail server with bad reputation</td>
<td>The mail routing path contains mail server with bad reputation (&lt;IP_address&gt;).</td>
</tr>
<tr>
<td>Significant time gap during email message transit</td>
<td>Significant time gap (&lt;duration&gt;) detected during email message transit between hops (&lt;source&gt; &amp; &lt;destination&gt;) from time (&lt;date_time&gt;) to time (&lt;date_time&gt;).</td>
</tr>
<tr>
<td>Inconsistent recipient accounts</td>
<td>Envelope recipient (&lt;email_address&gt;) is inconsistent with header recipient (&lt;email_address&gt;).</td>
</tr>
<tr>
<td>Possibly forged sender account or unexpected relay/forward</td>
<td>Possibly forged sender account (&lt;email_address&gt;) is sending email messages via host/IP (&lt;host_address&gt;) of which ASNs (&lt;ASN_list&gt;) are inconsistent to sender ASNs (&lt;ASN_list&gt;); or unexpected server-side</td>
</tr>
<tr>
<td>Email Characteristics</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Email message travels across multiple time zones</td>
<td>The email message travels across time zones (&lt;time_zone_list&gt;).</td>
</tr>
<tr>
<td>Possible social engineering attack characterized by suspicious charsets in email entities</td>
<td>Suspicious charsets (&lt;character_set_list&gt;) are identified in a single email message, implying the email message originated from a foreign region. This behavior is an indicator of a social engineering attack.</td>
</tr>
<tr>
<td>Violation of time headers</td>
<td>Multiple time headers (&lt;date_time&gt;, &lt;date_time&gt;) exist in one message, which violates RFC5322 section 3.6.</td>
</tr>
<tr>
<td>Possibly forged sender (Yahoo)</td>
<td>The email message claimed from Yahoo (&lt;email_address&gt;) lost required headers.</td>
</tr>
<tr>
<td>Executable files with tampered extension names in the attachment</td>
<td>Executable files in compressed attachment (&lt;file_name&gt;) intend to disguise as ordinary files with tampered extension names.</td>
</tr>
<tr>
<td>Anomalous relationship between sender/recipient(s) related email headers</td>
<td>Anomalous relationship between sender/recipient(s) related email headers (&lt;email_address&gt;).</td>
</tr>
<tr>
<td>Encrypted attachment intends to bypass antivirus scan engines</td>
<td>Encrypted attachment (&lt;file_name&gt;) with password (&lt;password&gt;) provided in email content possibly intends to bypass antivirus scan engines.</td>
</tr>
<tr>
<td>Email attachment could be exploitable</td>
<td>Email attachment (&lt;file_name&gt;) could be exploitable.</td>
</tr>
<tr>
<td>Email message might be sent from a self-written mail agent due to abnormal transfer encoding in email entities</td>
<td>Content-Transfer-Encoding (&lt;encoding_type&gt;) is abnormal in the email message. The email message might be sent from a self-written mail agent.</td>
</tr>
<tr>
<td>Few meaningful words in the email message</td>
<td>The email message is less meaningful with only few characters in its text/HTML body (&lt;character_count&gt;).</td>
</tr>
<tr>
<td>Possible email spoofing</td>
<td>The email message was claimed as a forwarded or replied message with subject-tagging (&lt;email_subject&gt;), but the email message does not contain corresponding email headers (RFC 5322).</td>
</tr>
<tr>
<td>Email message travels across multiple ASNs</td>
<td>The email message travels across multiple ASNs (&lt;ASN_list&gt;).</td>
</tr>
<tr>
<td>Email message travels across multiple countries</td>
<td>The email message travels across multiple countries (&lt;country_code_list&gt;).</td>
</tr>
<tr>
<td>Abnormal Content-type behavior in email message</td>
<td>Content-type in email content should not have attributes (&lt;attribute_list&gt;).</td>
</tr>
<tr>
<td>Executable files archived in the compressed attachment</td>
<td>Executable files archived in compressed attachment (&lt;file_name&gt;).</td>
</tr>
<tr>
<td>Exploitable file types detected in the compressed attachment</td>
<td>Exploitable file types detected in compressed attachment (&lt;file_name&gt;).</td>
</tr>
</tbody>
</table>
5.8 Understanding Policy Events

This screen enables you to track the email messages that trigger the advanced threat policy.

Trend Micro Hosted Email Security maintains up to 30 days' logs for policy events.

Queries include data for one day only. Use more than one query to search across calendar months. The Policy Event Query screen provides the following search criteria:

- **Type**
  - Advanced persistent threat: Query the messages that triggered the advance threat policy
    - All: query all messages
    - Analyzed Advanced Threats: Query the messages that are identified as threats according to advanced analysis 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 for advanced analysis due to exceptions that occurred during the analysis.
  - 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.
  - Message ID: The sender message ID.

When you query the email policy event, Hosted 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.

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 wildcard character at the same time.

The following policy event information is displayed:

- **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.

• Trigger Reason: The reason for the policy rule to trigger.

• Risk Rating: The risk rating of the message identified after advanced analysis.

• Action: The action taken on the message. For all the actions, see Actions below.
  - BCC: A blind carbon copy (BCC) was sent to the authorized recipients according to the Hosted Email Security policy.
  - Bypass: The message has been ignored and was not intercepted by Hosted Email Security.
  - Changed recipient: The recipient has been changed and the message has been redirected to a different recipient according to the Hosted Email Security policy established by the authorized mail administrator of this mail domain.
  - Clean: The message was cleaned for viruses by Hosted Email Security.
  - DeleteAttachment: The attachment in the email message has been deleted by Hosted Email Security.
  - Deliver: The message has been delivered to the downstream MTA that is responsible for transporting the message to its destination.
  - InsertStamp: A block of text was inserted into the email message body.
  - Message deleted: The message has been deleted by Hosted Email Security according to the policy established by the authorized mail administrator of this mail domain.
  - Notification: A notification was sent to the recipient when the policy rule was triggered.
  - Quarantined: Quarantined messages are blocked as detected spam or other inappropriate content before delivery to an email account. Messages held in quarantine can be reviewed and manually deleted or delivered.
  - TagSubject: Inserted a text defined in policy rules into the message subject line.
  - Encryption in progress: The message is being encrypted by Hosted Email Security. After encryption is complete, Hosted Email Security will queue the message for delivery.

• Scanned File Report (s): 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:**
If a file is detected as high-risk, Hosted Email Security will not send the file for advanced analysis, and therefore, a detailed report will not be available for such file. Reports could also be unavailable if an error occurs in generating the report.
If an email message contains multiple recipients, the result will be organized for each recipient separately.

5.9 Configuring Administration Settings

Do any of the following from the Administration screens:

- Manage administrator accounts for the Hosted Email Security server
  See Managing Administrator Accounts.

- Reset end user passwords for the Hosted Email Security End User Quarantine website
  See Changing End User Passwords.

- Upload user directories to Hosted Email Security for improved spam management
  See About Directory Management.

- Manage domain statuses in Hosted Email Security
  See About Domain Management.

- Co-brand and customize Hosted Email Security screens
  See About Co-Branding.

- Automate directory management in Hosted Email Security using web service clients
  See Installing Web Services.

- View the Hosted Email Security Service Level Agreement
  See Viewing Your Service Level Agreement.

5.9.1 Managing Administrator Accounts

5.9.1.1 About Account Management

Use the Administration > Account Management screen to search for accounts under your control and to act on behalf of those accounts.

After clicking Assume Control beside an account in the list, you will assume control of that account. For example, you will see and be able to change their Approved Senders and Blocked Senders lists, their Mail Tracking logs, and their managed domains on the Domain Management screens. You will also see the accounts they can control from their Account Management screen.

To stop acting on behalf of an account, click Release in the title bar area.
5.9.1.2 Adding and Configuring an Administrator Account

1. Go to Administration > Account Management.

2. Click Add. 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 predefined 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 OK.
   Hosted Email Security generates a password and sends it to the newly created account owner through an email message.

   **Note:**
   *If the account owner does not receive the notification message or deletes the notification message by mistake, you can resent the notification by clicking Send under the Send Email column on Account Management screen.*

   *The Send button will be disabled after the account owner logs in successfully.*

5.9.1.3 Editing Administrator Account Configuration

1. Go to Administration > Account Management.

2. Click on the account name that you want to edit.
   Edit Subaccount screen appears.

3. Modify the following information on the screen as required:
   - Subaccount Basic Information: modify the user Email Address.
     **Note:**
     *The user Account Name cannot be modified.*

   - Select Permission Types: select predefined permissions from the Predefined Permission Types list, or configure permissions for each of the feature manually.
   - Select Domains: select domains that the account can manage.

4. Click OK.
5.9.1.4 Deleting Administrator Accounts

1. Go to Administration > Account Management.

2. Select the accounts that you want to delete, and then click Delete.

3. Click OK on the confirmation dialog box.

5.9.1.5 Changing Administrator Passwords

**Note:**
If you have a Business account on the Customer License Portal (CLP), sign in to your Customer License Portal account and follow the instructions provided there.

Trend Micro recommends changing your password regularly.

You cannot change the password for a disabled account.

1. Go to Administration > Account Management.

2. Select the accounts for which you want to change passwords, and then click Reset Password.

Hosted Email Security generates new passwords for the accounts, and sends it to the account owners through an email message.

5.9.1.6 Enabling or Disabling an Administrator Account

1. Go to Administration > Account Management.

2. Click (enabled) or (disabled) to toggle the status of the account, and then click OK on the confirmation dialog box.

5.9.2 Changing End-User Passwords

If an end user loses their password, the system administrator can reset that password.

1. Go to Administration > End-User Passwords.

2. Type the managed email address of the end user.

3. Type and confirm the new password to be associated with the account.

**Important:**
Passwords must contain 8 to 32 alphanumeric characters. Trend Micro recommends using a long password. Strong passwords contain a mix of letters, numbers, and special characters.
5.9.3 About End-User Managed Accounts

End-users can manage multiple Hosted Email Security End User Quarantine website accounts by using a single account to log on. After an end-user begins managing an account, they can view the quarantined messages and set the Approved Senders associated with that account.

End-users log on with their primary account, and then specify one of their managed accounts or All managed accounts at the top of the screen to view Quarantined messages and set Approved Senders for the specified account or accounts.

Figure 1. Example of the End-User Managed Account Selection Control

After an end-user begins managing an account, that managed account will be unable to log on to the End User Quarantine website. The managed account will be able to log on again only if the account management relationship is removed. To allow the account to log on again, the primary account can remove the managed account from the Managed Accounts screen of the End User Quarantine website.

Adding a managed account does not change the credentials for that account.

The Hosted Email Security administrator console allows you to enable or disable (enabled by default) the ability of users to add managed accounts. Disabling the feature does not change the account management relationship of accounts that end-users have already added.

Tip: The toggle button shows the current enabled or disabled state of the setting. Click the button to switch the state of the setting.

End-users can always remove accounts from their list of managed accounts. However, end-users can only add management of accounts under the following conditions:

- The Hosted Email Security administrator has enabled the feature.
- The account is a registered End User Quarantine website account.
- The account is not currently a managed account of another End User Quarantine website account.
- The end-user is able to open the confirmation email message sent to the account address.
- The end-user has the End User Quarantine website password for the account.
5.9.3.1 Removing End-User Managed Accounts

The primary account can remove the managed account from the Managed Accounts screen of the End User Quarantine website.

To remove an account management relationship using the Hosted Email Security administrator console, use the following procedure.

1. Go to the End-User Managed Accounts screen.
2. Select the primary account and managed account pair or pairs in the list.
3. Click Remove.

5.9.4 About Directory Management

You can import LDAP Data Interchange Format (LDIF) or comma-separated values (CSV) files into Hosted Email Security. This helps Hosted Email Security to better filter and process messages for valid email addresses. Messages to invalid email addresses will be rejected.

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

Hosted Email Security also provides a Synchronization Tool that enables you to synchronize your current groups and email accounts on the ActiveDirectory server with the Hosted Email Security server.

The Directory Management screen includes the following tabs:

- Directory Import
  - Import User Directory: Selections for importing a new user directory file
  - Imported User Directories: The current user directory file(s) that Hosted Email Security is using

- Directory Synchronize
  - Synchronization Summary: Displays the number of valid recipients and groups synchronized using the synchronization tool.
  - Synchronization History: Displays the last seven (7) days' synchronization history.
5.9.4.1 Importing User Directories

You can import LDAP Data Interchange Format (LDIF) or comma-separated values (CSV) files into Hosted Email Security. This helps Hosted Email Security to better filter and process messages for valid email addresses. Messages to invalid email addresses will be rejected.

**Important:**
Before you import an LDIF or CSV directory file, note the following:

- Hosted Email Security only recognizes ANSI-encoded LDIF (with the extension .ldf) and ANSI or UTF-8-encoded CSV (with the extension .csv) files. Do not include blank lines or other irrelevant data in the file that you import. Use caution when creating a file.

- When importing user directory files, Hosted Email Security replaces all records for a managed domain at once. If any email addresses for a managed domain are imported, all other email addresses for that domain are removed. Newly imported email addresses for that domain, and records for other managed domains, will be kept. If you import an updated user directory file that does not have any information for one of your domains, the entries for those domains remain the same and are not overwritten.

- Every time you import a directory file, it overwrites the old version. If you import an updated directory file that has information for one of your domains, all entries for those domains are overwritten. Use caution when importing a directory.

- You can only see the directories that are associated with your administrator account. If you are sharing your Hosted Email Security service with another administrator (for example, a value-added reseller) who logs on with his/her specific account information, Hosted Email Security will not show the directories for that account.

- Every time you add more users to your network, you must import your updated user directories; otherwise, Hosted Email Security will reject email from newly added users.

**Warning:**
Trend Micro strongly suggests that you do not import more than 24 directories in a day. Doing so could overwhelm system resources.

1. Next to Format, select the format type:
   - LDIF
   - CSV
**Important:** If you create a CSV file, divide the records into fields for email_address and Firstname Lastname and separate them using a comma and optional quotation marks. Use of spaces or other delimiters is not supported. Use one record per line.

For example:

<table>
<thead>
<tr>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:bob@example.com">bob@example.com</a>,Bob Smith</td>
</tr>
<tr>
<td><a href="mailto:sally@example.com">sally@example.com</a>,Sally Jones</td>
</tr>
<tr>
<td>&quot;<a href="mailto:bob@example.com">bob@example.com</a>&quot;,&quot;Bob Smith&quot;</td>
</tr>
<tr>
<td>&quot;<a href="mailto:sally@example.com">sally@example.com</a>&quot;,&quot;Sally Jones&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Not Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:bob@example.com">bob@example.com</a>,Bob Smith,<a href="mailto:sally@example.com">sally@example.com</a>,Sally Jones</td>
</tr>
</tbody>
</table>

Microsoft Excel will save a two column chart as a CSV using valid formatting.

2. Next to Name, type a descriptive name for the file.

3. Next to File location, type the file directory path and filename or click Choose File and select the .ldf or .csv file on your computer.

4. Click Verify File to read the file and show a summary of how many email addresses were found. After the progress bar completes, a summary screen appears showing the following:
   - **Summary:** A summary of the information above
   - **Domains and Number of Current Users to Replace Current Users:** The domains that you specified when you subscribed to the Hosted Email Security service
   - **Invalid domains:** Any domains that are included in your directory file, but are not officially registered with your Hosted Email Security service

5. Click Import. This will import and then enable the email address list.

**Note:**

You can verify which email addresses were found by selecting your domain name and clicking the Export to CSV button.

If you need to disable the feature, you can click the toggle.

The toggle button shows the current enabled 

or disabled state of the setting. Click the button to switch the state of the setting.
5.9.4.2  Synchronizing User Directory

- The Directory Synchronize tab displays synchronization summary and history. The screen is divided into two sections:

- Synchronization Summary: This section displays the number of valid recipients and groups synchronized using the synchronization tool.

- Synchronization History: This section displays the last seven (7) days' synchronization history. It includes the following information:
  - Synchronization time
  - Type: whether the synchronized data includes valid recipients, groups or both
  - the synchronization tool information including the machine's IP address or hostname where the tool is installed
  - synchronization result: whether the synchronization is successful or unsuccessful, or whether any groups or policies were added or removed.

5.9.4.3  Verifying UserDirectories

If you are uncertain which domains in the user directories are going to be active for your service, you can temporarily disable the directories, import the file, export the directories to a CSV file, and view them without the directory being enabled. When you are confident that the user directory is correct, you can re-enable it.

**Note:**
Hosted Email Security takes up to five minutes to enable or disable the directories.

Verifying User Directories for Valid Recipients

1. Disable the Valid recipient check.

   **Note:**
   The toggle button shows the current enabled [✓] or disabled [✗] state of the setting. Click the button to switch the state of the setting.

2. Import directories or synchronize valid recipients.

3. Select the domains from the Valid recipient drop-down list that you want to verify.

4. Click Export to CSV for Valid recipient.

5. Save the directory file.

6. Open the directory file in an application that reads CSV files.

7. Verify that the recipient information is correct.

8. Re-enable the Valid recipient check.
Verifying User Directories for Directory Groups

Note: Perform this procedure after you have synchronized user groups using Synchronization Tool.

1. Select the groups from the Directory groups drop-down list that you want to verify.
2. Click Export to CSV for Directory groups.
3. Save the group file.
4. Open the group files in an application that reads CSV files.
5. Verify that the group information is correct.

5.9.5 About Domain Management

Use the Administration > Domain Management screen to add, modify, or deactivate domains.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound Server(s)</td>
<td>IP address or FQDN: Fully qualified domain name (FQDN) is a unique name, which includes both host name and domain name, and resolves to a single IP address.</td>
</tr>
<tr>
<td></td>
<td>• For example: hostmaster1.example.com or mailhost.example.com</td>
</tr>
<tr>
<td></td>
<td>• Not valid: example.com</td>
</tr>
<tr>
<td></td>
<td>Port: Port is a number from 0-65535 that an inbound server listens on. These ports vary based on server configuration. Well-known ports for email servers include SMTP at 25, SMTPS at 465, and MSA at 587.</td>
</tr>
<tr>
<td></td>
<td>Preference: Preference, sometimes referred to as distance, is a value from 1 to 100.</td>
</tr>
</tbody>
</table>

Note: If more than one mail server is available, delivery is prioritized to servers with lower values. Using the same value will balance delivery to each server.

<table>
<thead>
<tr>
<th>Outbound Server(s)</th>
<th>If outbound filtering is enabled, this is the information for the MTA(s) that Hosted Email Security relays your outbound messages from. The following choices are available:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use Office 365: Relays your outbound messages from your Office 365 solution</td>
</tr>
</tbody>
</table>
Table 1. Activate a Domain Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Google Apps:</td>
<td>Relays your outbound messages from your Google Apps solution</td>
</tr>
<tr>
<td>Specify IP address(es):</td>
<td>Relays your outbound messages from the specified IPv4 address(es) for your</td>
</tr>
<tr>
<td></td>
<td>current MTA(s)</td>
</tr>
<tr>
<td>Seat count</td>
<td>This is the licensed seat count used by this domain. Seats correspond to</td>
</tr>
<tr>
<td></td>
<td>the number of actual email users in the domain.</td>
</tr>
<tr>
<td>Send test message to</td>
<td>Optional email address used to confirm email delivery from Hosted Email</td>
</tr>
<tr>
<td></td>
<td>Security. Manually send test messages to this address from the Domain</td>
</tr>
<tr>
<td></td>
<td>Management screen.</td>
</tr>
</tbody>
</table>

Domain status is shown in the Domains table at the bottom of the screen. Domain status can be one of the following:

Table 2. Domain Status Descriptions

<table>
<thead>
<tr>
<th>Domain Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding</td>
<td>Hosted Email Security is waiting for you to point your MX record to the</td>
</tr>
<tr>
<td></td>
<td>Hosted Email Security MTA for your region</td>
</tr>
<tr>
<td>Activated</td>
<td>Domain is successfully delivering email messages</td>
</tr>
</tbody>
</table>

5.9.5.1 Adding a Domain

1. Type the information for your current MTAs or mail servers in the following fields:

   **Note:**
   You can specify up to 30 inbound servers and 30 outbound servers. Use the add and the remove buttons to manage additional entries.

   - Domain name: Includes everything to the right of the at sign (@) in email addresses managed by the server(s) being activated
   - Seat count: Seats correspond to the number of actual email users in the domain
   - Inbound server(s)
     - IP address or FQDN: Fully qualified domain name (FQDN) is a unique name, which includes both host name and domain name, and resolves to a single IP address.
     - Port: Port is a number from 0-65535 that an inbound server listens on. These ports vary based on server configuration. Well-known ports for email servers include SMTP at 25, SMTPS at 465, and MSA at 587.
     - Preference: Preference, sometimes referred to as distance, is a value from 1 to 100.

   **Note:**
   If more than one mail server is available, delivery is prioritized to servers with lower values. Using the same value will balance delivery to each server.
Optionally, select Enable outbound filtering and refer to the following table:

**Warning:**

*Enabling outbound filtering without specifying outbound servers will prevent the delivery of any outbound traffic routed through the service.*

### Steps to Configure Outbound Filtering

<table>
<thead>
<tr>
<th>Email Solution</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>You currently use Office 365</td>
<td>Select Use Office 365.</td>
</tr>
<tr>
<td>You currently use Google Apps</td>
<td>Select Use Google Apps.</td>
</tr>
</tbody>
</table>
| You do not use Office 365 or Google Apps | Select Specify IP address(es).  
                                        | Type the IP address(es) of your outbound server(s). |

- Send test message to: Optional email address used to confirm email delivery from Hosted Email Security. Manually send test messages from the Domain Management Details screen.

To display the Domain Management Details screen, follow the step to edit information for a domain at Managing Domains.

2. **Click Activate Domain.**

If the domain is valid and an MX record for the domain exists, the domain appears in the Domains table at the bottom of the screen.

Trend Micro sends a welcome message to the administrative email address on record confirming that your domain has been added successfully and stating: "This welcome message confirms your domain has been successfully added."

**Warning:**

*Do not repoint your MX record until you receive the message confirming that your domain has been added. The administrative email address on record should receive the welcome message, which is that confirmation. If you repoint your MX record before your domain has been successfully added, your email messages may be lost.*

3. If you currently use Office 365, you can configure Office 365 connectors to allow email traffic to or from Hosted Email Security MTAs.

See Adding Office 365 Inbound Connectors.

See Adding Office 365 Outbound Connectors.

See Repointing MX Records (Best Practice)
5.9.5.2 Managing Domains

1. Select domains by doing one of the following:
   - To select one or more domains, select the check boxes to the left of each entry.
   - To select all domains, select the check box to the left of the Domain Name column title.

2. Manage selected domains by clicking one of the following buttons:
   - Deactivate: Submit a deactivation request to Trend Micro for action
   - Check MX Record: Verify the MX record points to the Hosted Email Security inbound MTA

3. To edit information for a domain, do the following:
   a. Click the domain name in the Domains list at the bottom of the Domain Management screen. The Domain Management Details screen appears, displaying the title Domain Management > {your-domain-name} with fields pre-filled with the information on record for that domain.
   b. Modify the fields as needed.

5.9.5.2.1 Enabling Outbound Filtering for a Domain

1. Follow the steps to open the Domain Management Details screen for your managed domain.
   To display the Domain Management Details screen, follow the step to edit information for a domain at Managing Domains.

2. Enable Outbound Filtering for your managed domain.
   Select Enable outbound filtering and refer to the following table:

   Warning: Enabling outbound filtering without specifying outbound servers will prevent the delivery of any outbound traffic routed through the service.

   Table 1. Steps to Configure Outbound Filtering

<table>
<thead>
<tr>
<th>Email Solution</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>You currently use Office 365</td>
<td>a. Select Use Office 365.</td>
</tr>
<tr>
<td></td>
<td>Tip: If you use Office 365, configure Office 365 connectors to allow email traffic from Hosted Email Security MTAs. See Adding Office 365 Outbound Connectors.</td>
</tr>
<tr>
<td>You currently use Google Apps</td>
<td>a. Select Use Google Apps.</td>
</tr>
<tr>
<td>You do not use Office 365 or Google Apps</td>
<td>a. Select Specify IP address(es).</td>
</tr>
<tr>
<td></td>
<td>b. Type the IP address(es) of your outbound server(s).</td>
</tr>
</tbody>
</table>
5.9.6 About Co-Branding

Hosted Email Security enables you to display a service banner, such as your company logo, on the top banner of the Hosted Email Security logon screen, administrator console, and End User Quarantine website. You can set different domains with the same or different service banners or can allow domain administrators to set the service banner to be displayed for their domain. You can also leave the feature disabled.

The following is an example of a customized service banner:

![Hosted Email Security](image)

The service banner selected for a domain will display in the top banner of the Hosted Email Security logon screen, the Hosted Email Security End User Quarantine website, and the administrator console associated with that domain. The service banner selected for an account name will display only in the Hosted Email Security administrator console.

**Note:**

Co-branding is disabled by default.

The toggle button shows the current enabled or disabled state of the setting. Click the button to switch the state of the setting.

Resellers can set different service banners for different domains or allow system administrators of the domain to set the service banner for that domain.

Before attempting to establish co-branding, verify that your service banner image meets the following requirements:

<table>
<thead>
<tr>
<th>Table 1. Service Banner Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image Attributes</strong></td>
</tr>
<tr>
<td>Height</td>
</tr>
<tr>
<td>Width</td>
</tr>
<tr>
<td>File format</td>
</tr>
</tbody>
</table>
5.9.6.1  Accessing the Co-Branded Administrator Console and End User Quarantine Website

As a reseller, you can supply your customers with a web address they can use to access their co-branded Hosted Email Security administrator console and End User Quarantine website.

**Note:**
If an end user accesses a co-branded website without appending the account name or domain name, the website will still use co-branding for all screens except the logon screen.

Refer to the access locations for your region in the table below:

<table>
<thead>
<tr>
<th>Console or Website</th>
<th>Steps for Europe, the Middle East, Africa</th>
<th>Steps for All Other Regions</th>
</tr>
</thead>
</table>
| Administrator console for Customer Licensing Portal (CLP) Business accounts | Append /co-brand/ and the Hosted Email Security account name to the base URL. For example:  
  - Hosted Email Security administrator console: [https://tm.hes.trendmicro.eu](https://tm.hes.trendmicro.eu)  
  - Co-branded administrator console for the account named "adminA": [https://tm.hes.trendmicro.eu/co-brand/adminA](https://tm.hes.trendmicro.eu/co-brand/adminA) | Append /co-brand/ and the Hosted Email Security account name to the base URL. For example:  
  - Hosted Email Security administrator console: [https://tm.hes.trendmicro.com](https://tm.hes.trendmicro.com)  
  - Co-branded administrator console for the account named "adminA": [https://tm.hes.trendmicro.com/co-brand/adminA](https://tm.hes.trendmicro.com/co-brand/adminA) |
| Administrator console for xSP and local accounts | Append /co-brand/ and the Hosted Email Security account name to the base URL. For example:  
  - Hosted Email Security administrator console: [https://ui.hes.trendmicro.eu](https://ui.hes.trendmicro.eu)  
  - Co-branded administrator console for the account named "adminB": [https://ui.hes.trendmicro.eu/co-brand/adminB](https://ui.hes.trendmicro.eu/co-brand/adminB) | Append /co-brand/ and the Hosted Email Security account name to the base URL. For example:  
  - Hosted Email Security administrator console: [https://ui.hes.trendmicro.com](https://ui.hes.trendmicro.com)  
  - Co-branded administrator console for the account named "adminB": [https://ui.hes.trendmicro.com/co-brand/adminB](https://ui.hes.trendmicro.com/co-brand/adminB) |
| End User Quarantine website | Append /euq-co-brand/ and the Hosted Email Security managed domain to the base URL. For example: | Append /euq-co-brand/ and the Hosted Email Security managed domain to the base URL. For example: |

Note: If an end user accesses a co-branded website without appending the account name or domain name, the website will still use co-branding for all screens except the logon screen.
### Table 1. Access Locations

<table>
<thead>
<tr>
<th>Console or Website</th>
<th>Steps for Europe, the Middle East, Africa</th>
<th>Steps for All Other Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> This applies to Customer Licensing Portal, xSP, and local accounts.</td>
<td>Hosted Email Security End User Quarantine website: <a href="https://euq.hes.trendmicro.eu">https://euq.hes.trendmicro.eu</a> Co-branded administrator console for the managed domain &quot;example.com&quot;: <a href="https://euq.hes.trendmicro.eu/euq-co-brand/example.com">https://euq.hes.trendmicro.eu/euq-co-brand/example.com</a></td>
<td>Hosted Email Security End User Quarantine website: <a href="https://euq.hes.trendmicro.com">https://euq.hes.trendmicro.com</a> Co-branded administrator console for the managed domain &quot;example.com&quot;: <a href="https://euq.hes.trendmicro.com/euq-co-brand/example.com">https://euq.hes.trendmicro.com/euq-co-brand/example.com</a></td>
</tr>
</tbody>
</table>

### 5.9.7 Installing Web Services

Hosted Email Security Web Services automate some repetitive tasks. The Web Services Client and Active Directory Synchronization Tool automate the import of directory files of valid recipient email addresses. The Active Directory Synchronization Tool also enables you to import user groups. The Web Services Client and Active Directory Synchronization Tool functionally is similar to the Import User Directory feature on the Directory Management screen.

1. Go to Administration > Web Services.
2. If Current Key under Service Authentication Key is blank, click Generate New Key to generate a key. The Service Authentication Key is the global unique identifier for your Web Service Client to authenticate its access to Hosted Email Security Web Services.

**Important:**

Current Key displays the Service Authentication Key that the Web Services Client should use. If you generate a new key, you must update Web Services Client to use the new key. The Service Authentication Key allows your Web Services Client to communicate with Hosted Email Security Web Services. Keep the Service Authentication Key private.

3. Enable Applications using the button at the right of the screen (disabled by default).

**Tip:**

The toggle button shows the current enabled or disabled state of the setting. Click the button to switch the state of the setting.

4. In the Downloads list, click download to download the desired items. Download the Web Services Guide for additional instructions on the use and configuration of Hosted Email Security Web Services.

- Active Directory Synchronization Tool: For synchronizing accounts and groups between local Active Directory and Hosted Email Security server
- Active Directory Synchronization Tool User Guide: For more information on using the synchronization tool
- Web Services Client: For most environments
5. Save the client on a local drive.

6. Follow the client installation steps to install the client.

5.9.8 Viewing Your Service Level Agreement

Trend Micro provides a Service Level Agreement (SLA) for Hosted Email Security that is intended to help your organization receive secure, uninterrupted email service.

The Service Level Agreement covers availability, latency, spam blocking, false positives, antivirus, and support. Specific service-level guarantees are included in the most current version of the Hosted Email Security Service Level Agreement, which you can view or download from this screen.

**Important:**

Provisions of the Service Level Agreement may vary among regions, so be sure to select your region and language when using this screen. Trend Micro reserves the right to modify the service at any time without prior notice. The current version of the Hosted Email Security service level agreement is available for review by paid customers and by customers conducting a trial.

To view the Service Level Agreement for your region:

1. Go to Administration > Service Level Agreement. The Hosted Email Security Service Level Agreement screen appears.

2. In the drop-down list, select your language/region.

**Tip:**

Disable any pop-up blockers for your browser in order to download the Service Level Agreement.

Hosted Email Security displays an Adobe Reader (PDF) document of the Service Level Agreement for the language and region that you selected.