Table of Contents

**Product Description** ........................................................................................................... 5
  1.1 Mail Flow ............................................................................................................................ 6
    1.1.1 Inbound Scanning ......................................................................................................... 6
    1.1.2 Outbound Scanning ..................................................................................................... 6
  1.2 Levels of Service ............................................................................................................... 7
    1.2.1 Hosted Email Security – Inbound Filtering ................................................................. 7
    1.2.2 Hosted Email Security (Full Version) ......................................................................... 7
  1.3 Hosted Email Security Web Console (Administrative Console) ........................................ 8
  1.4 Hosted Email Security Editions ....................................................................................... 9

**Preparation** ....................................................................................................................... 10
  2.1 Prerequisites ..................................................................................................................... 10
  2.2 Software Required for Accessing Your Account ........................................................... 11
  2.3 Default Hosted Email Security Settings .......................................................................... 11

**Getting Started** .................................................................................................................. 12
  3.1 Registering and Activating Hosted Email Security ......................................................... 12
    3.1.1 Registration (New Customers) ...................................................................................... 12
    3.1.2 Registration (Renewing Customers or Upgrading from Trial) .................................... 12
    3.1.3 Activation ................................................................................................................... 13
    3.1.4 Message Test .............................................................................................................. 15
  3.2 MX Redirection .................................................................................................................. 17
  3.3 Other Scenarios ................................................................................................................ 18
    3.3.1 Switching from 3rd Party solutions ............................................................................ 18
    3.3.2 Multiple IP Addresses ............................................................................................ 19

**Recommended Settings** ..................................................................................................... 20
  4.1 Policy .................................................................................................................................. 20
  4.2 Approved senders .............................................................................................................. 20
  4.3 IP Reputation .................................................................................................................... 20
  4.4 Directory Management ..................................................................................................... 20
    4.4.1 AD Sync client .......................................................................................................... 21
WEB EUQ.......................................................................................................................... 22

5.1 Accessing the Web End User Quarantine ........................................................................... 22
   5.1.1 Creating an Account .................................................................................................. 22
   5.1.2 Logging on to Hosted Email Security Web End User Quarantine ......................... 23

5.2 Managing Quarantined Spam.............................................................................................. 23

Spam Prevention ....................................................................................................................... 25

6.1 Securing your Mail Server.................................................................................................. 25
6.2 Securing your Users/Customers.......................................................................................... 26
6.3 Securing with HES.............................................................................................................. 26

About Trend Micro™ .................................................................................................................. 28
Chapter 1

Product Description

Trend Micro Hosted Email Security delivers high-performance, cost-effective hosted security services, protecting businesses against spam, viruses, and inappropriate content before they reach their network.

Hosted Email Security works by intercepting customer mails via mail exchange (MX) record redirection to HES inbound mail transfer agent servers.

HES has a selection of configurable policies to fit customer organization's email security requirements.

HES customers are secured using two main tiers of security protection - Email Reputation Service (connection-level reputation based filtering) and Email Content-based Filtering using Trend Micro Anti-Spam Engine and most up-to-date spam patterns.
1.1 Mail Flow

1.1.1 Inbound Scanning

1. The originating mail server performs a DNS lookup to determine the location of the example.com domain. The Mail exchange (MX) record for example.com holds the IP address of Hosted Email Security instead of the original IP address for example.com, since Hosted Email Security must first scan your company’s mail before final delivery to your local email server.

2. The originating mail server routes the mail to Hosted Email Security.

3. Hosted Email Security servers accept the message and perform message filtering and policy matching on your behalf.

4. Assuming that a message is slated for delivery according to its security policy or validity status, the Hosted Email Security servers route the message to the original example.com mail servers.

1.1.2 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.

1.2 Levels of Service

Hosted Email Security is available in two basic levels of service:

1.2.1 Hosted Email Security – Inbound Filtering

This service level provides several default settings to provide immediate protection upon deployment. In this version, only the spam action can be changed, minimizing the administration needed.

1.2.2 Hosted Email Security (Full Version)

The full version provides robust management options, enabling you to customize your threat protection and set email use policies to meet the needs of your organization. The features unique to this service level include the following:

- Content filtering

- Email Encryption (a separate, add-on service available for purchase)

- Customized threat and outbound email filtering (optional)
Email Encryption

Trend Micro Email Encryption for outbound mail is an add-on service to Hosted Email Security (full version) that is available for purchase. Email Encryption is seamlessly integrated with the content-filtering capabilities of Hosted Email Security. The service does not automatically encrypt email. When enabled, Email Encryption appears as a rule enforcement option within the Hosted Email Security administrative console. You will need to configure rules that apply encryption as a rule action.

In order to use the email encryption service, you must first deploy Hosted Email Security (full version) with outbound filtering.

1.3 Hosted Email Security Web Console (Administrative Console)

The Hosted Email Security Web console enables mail administrators to create reports, view logs, perform administrative tasks, and set or alter policies (full version customers only).
1.4 Hosted Email Security Editions

This service is offered in the following editions:

<table>
<thead>
<tr>
<th>INBOUND FILTERING VERSION</th>
<th>FULL VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Antivirus and IP connection spam prevention</td>
<td></td>
</tr>
<tr>
<td>• Heuristic, content-based spam prevention filter</td>
<td></td>
</tr>
<tr>
<td>• Default anti-virus policies cannot be changed (read-only)</td>
<td></td>
</tr>
<tr>
<td>• Access to reports, mail tracking, and password administration</td>
<td></td>
</tr>
<tr>
<td>• End-user quarantine with configurable quarantine digest notification email</td>
<td></td>
</tr>
<tr>
<td>• Outbound message filter</td>
<td></td>
</tr>
<tr>
<td>• Content filtering for corporate compliance</td>
<td></td>
</tr>
<tr>
<td>• Ability for administrator to create custom policies (create and modify rights)</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 2

Preparation

Hosted Email Security is a hosted service, and does not require additional hardware (other than your mail gateway) on your premises. All scanning hardware is off-site at secure Trend Micro network operations centers. The service is managed by security professionals, relieving your IT staff the burden of installing, maintaining, and fine-tuning a complex email security system.

To access your web-based Hosted Email Security administration account, you need a personal computer with connection to the Internet.

2.1 Prerequisites

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

- An existing Internet gateway or workgroup SMTP connection
- Access to the DNS mail exchange record, to redirect the MX mail host record (Contact your service provider, if necessary, for more information or configuration help.)

Important:

Do not redirect your MX record until you receive confirmation that your account has been established. If you redirect your MX record before your account is set up, your email may be lost. Redirection details will be provided by Trend Micro.
2.2 Software Required for Accessing Your Account

To access your account, you need Internet access and one of the following recommended browsers with the latest Java Script™ installed:

- Microsoft™ Internet Explorer™ 6.0, 7.0, or 8.0
- Mozilla™ Firefox™ 2.0 and above

2.3 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:
Chapter 3

Getting Started

3.1 Registering and Activating Hosted Email Security

3.1.1 Registration (New Customers)

Hosted Email Security customers need to register an account before using the service. The log in information that will be created thru this process will be their log in credentials in accessing Hosted Email Security web console.

To create an account, you can follow the instructions on the link below:

3.1.2 Registration (Renewing Customers or Upgrading from Trial)

Hosted Email Security customers who renewed their account or upgraded from trial version, will receive a registration key. They need to register this key on their existing Trend Micro account.

To register, you can follow the instructions on the link below:
3.1.3 Activation

1. Using the provided **On-line Registration** (OLR) username and password, log on to the HES console:

   - For US: [https://us.emailsec.trendmicro.com/loginPage.imss](https://us.emailsec.trendmicro.com/loginPage.imss)
   - For EMEA: [https://emailsec.trendmicro.eu/loginPage.imss](https://emailsec.trendmicro.eu/loginPage.imss)

   **Important:** Make sure that the Log on with Trend Micro Online Registration user name and password checkbox is ticked.

2. Enter your domain and IP information, and then click **Add Domain**

   ![Add Domain Form]

   3. Once your managed domain list is complete, tick the checkbox beside your managed domain and click **Submit**

   4. You will be notified that your activation request has been sent. Wait for your welcome email. This will take 48 hours at most. The welcome email will guide you through the final steps needed.
before starting the service. Moreover, it contains the HES/HES - Inbound Filtering MX records you will need for your account

5. While waiting for your welcome email, it is advised to log on to HES console again. This is to verify that domain settings are correct. Domain status should show “Verifying”

**Important:**

*Do not change the MX records until the welcome email has been successfully received. If the welcome email was not received, please contact Trend Micro Technical Support.*

*When modifying MX records, the full transition (DNS propagation) may take up to 48 hours. During this time we recommend that you do NOT discontinue any on-premise security. You may still receive some email directly until the transition period is complete. For best practice, please see 3.2 below.*
3.1.4 Message Test

1. After modifying your MX record, and DNS propagation has completed, log on to HES console to check domain status

2. Once the domain shows "Activated", send a test email via the HES console
   a. Under Administration tab, select Domain Management
   b. Click the domain name you added
   c. Type the email address you would like to send the test email to, and then click Test
3. Check the test email

*Important:*

*It is advised to review all default policy. To check, go to HES console, then select the **Policy** tab.*
3.2 MX Redirection

When the newly added domain is in a "Verifying" state, it means that the domain's MX record is not yet redirected to HES.

To get the domain to "Activated" status, you need to point your MX record to HES. Once HES identifies that the MX record has been redirected to the service properly, the newly added domain will then enter the “Activated” state.

Below are the MX records for HES:

**Important:** You must **NEVER** use this as your MX record if your domain is not yet added in HES.

- EMEA: in.mx.trendmicro.eu
- Other Regions: in.sjc.mx.trendmicro.com

The best way to redirect your MX record to HES is to add HES as **SECONDARY** MX record with a lower priority. In this way, message flow will not be interrupted while waiting for full DNS propagation.

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

Once you’re done testing and would like to use HES full time, please delete your first MX record.

**Tip:** It is highly recommended that HES is the sole MX record of your domain. This is to force all emails to be scanned by HES and avoid direct spamming to your mail server.

To make sure that your domain's MX record is pointed to HES servers. To check, type the following on the command prompt:
3.3 Other Scenarios

3.3.1 Switching from 3rd Party solutions

If you are currently using other hosted mail scanning service and is now moving to HES, you might encounter an error when adding your domain on the web console.

The most frequent error is “The IP address entered does not match the mail server address of the domain. Verify the mail server and try again.” This happens because HES verifies the IP/FQDN that you entered when adding a domain matches its current MX record.

To solve this please follow these instructions:

1. Open a command prompt window
2. Type the following command, and then press Enter

```
nslslookup -q=mx <domain name>
```

The results will show the IP address for that specific MX record. You may now use this IP address to add your domain on the HES console.

If the MX record for the domain you are trying to add is pointed to the HES servers (this information can be found in your welcome email), you may do one of the following options:

**Option 1:** Revert to your original MX record since HES will not accept your domain activation request.

**Option 2:** Create a secondary MX record with a different priority and point it directly to your mail server.

*Important:*

*DNS propagation takes 24-48 hours globally; please wait for the MX record to be propagated before trying to add the domain again.*

### 3.3.2 Multiple IP Addresses

To ensure mail delivery, Hosted Email Security allows customers to point HES / HES - Inbound Filtering to more than one mail server.

To do so, you may follow the steps the link below:

Chapter 4

Recommended Settings

4.1 Policy

Set the actions of the rule/s Spam or Phish to Quarantine. This is to make sure that you can recover a valid email from a false positive detection.

4.2 Approved senders

Make sure that you only approved trusted email addresses or domains. Adding an email address or domain in the Approved Senders list will bypass Spam or Phish rules and IP Reputation scanning.

Important:

*Do not add your own domain in the approved sender’s list, this will allow spam to reach through your network.*

4.3 IP Reputation

Use the default setting, 2, which is a moderately tolerant setting. Trend Micro recommends that you make changes to the Dynamic Settings carefully and in small increments. You can then fine-tune your settings based on the increased amount of spam and legitimate messages received.

4.4 Directory Management
It is highly recommended to import **Valid Recipients** list and enable **Directory Management** feature. This will prevent **Directory Harvest Attack** on your mail server.

To know more about Directory Management and importing valid recipients, please see below link.  

### 4.4.1 AD Sync client

Customers using Active Directory may install AD sync client to retrieve the data from customer AD server and syncs the data over to the AD sync server. This is installed inside customer’s LAN while the server is in Trend Micro data center.

To avoid errors, please download the latest AD sync client installer in the HES console. It is located under Administration> Web Services. Also on that page make sure to enable the "Applications" (you will see a red X button along its line if disabled and a green check if enabled). Next go to Directory Management and make sure to enable “Imported User Directories”. Then you may now install the AD sync client. Please make sure that any previous versions of AD sync client are not installed on your server.

Please follow this knowledge base article on how to install AD sync client:  

Please follow this Technet article on how to get the correct LDAP path;  

Please follow this knowledge base article on how to configure the AD sync client:  

If AD Sync client was unable to sync all of your contacts, please follow this knowledge base article on how to solve it:  
Chapter 5

WEB EUQ

The Hosted Email Security Web End User Quarantine (EUQ) is a user interface that helps end users to manage spam email messages held in quarantine. End users can also set up a list of approved email senders whose messages should be delivered, not quarantined.

5.1 Accessing the Web End User Quarantine

To access the Web End User Quarantine, you need Internet access and one of the following recommended browsers:

- Microsoft™ Internet Explorer™ 6.0, 7.0, or 8.0
- Mozilla™ Firefox™ 2.0 and above

Users whose domains are registered to HES / HES - Inbound Filtering can create their individual accounts to manage spam by accessing any of the following:

For US: [https://us.emailsec-euq.trendmicro.com/](https://us.emailsec-euq.trendmicro.com/)

For EMEA: [https://emailsec-euq.trendmicro.eu/](https://emailsec-euq.trendmicro.eu/)

5.1.1 Creating an Account

5.1.2 Logging on to Hosted Email Security Web End User Quarantine

After creating a new account, you will receive an email message notifying you that your information has been authenticated and that your account has been created.

To log on to Web End User Quarantine for the first time, you may follow the instructions on the link below:


5.2 Managing Quarantined Spam

Trend Micro Web EUQ only maintains quarantined messages up to 21 days in EMEA region and 15 days in all other regions. These messages would be subsequently deleted so it is recommended to check and manage your quarantined spam regularly.
The quarantined spam is the first screen you see when you log on to Web EUQ. To manage your quarantined spam, you can view and sort quarantined items in the table, and/or you can perform one of the three actions for quarantined items.
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.

### 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.


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.
4. Disable all open mail relay on your network

6.2 Securing your Users/Customers

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.

6.3 Securing with HES

1. Enable outbound scanning
   This option is only applicable for users with the full version of HES. Make sure also to enable most if not all of your outbound policies in the web console.

2. Enable Directory Management
   This is to ensure that only legitimate users from your network are allowed to receive inbound emails for your domain. If you’re using Active Directory then you may use the AD sync client to automatically export your users to HES. If not, you can just upload a CSV file of all of your users’ email addresses.

3. Use the HES policies
   It will be best to enable as much policies as possible (in HES console) if not all. This is to ensure that all filters are used to scan the email before it goes to your server. Limit the use of wildcards for the domains you except on the policies, and as much as possible just except email addresses so this way not all emails for that domain will just pass through the policy.
4. Submit undetected spam mails

If you still receive spam mails, gather the actual spam samples in MSG or EML format and compress them in a password-protected ZIP file (password: novirus).

Submit the compressed samples to spam@supporttrendmicro.com.
Trend Micro, Incorporated is a global leader in network antivirus and Internet content security software and services, focused on helping customers prevent and minimize the impact of network viruses and mixed-threat attacks through its award-winning Trend Micro Enterprise Protection Strategy. Trend Micro has worldwide operations and trades stock on the Tokyo Stock Exchange and NASDAQ.

Copyright © 2012 by Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, and Worry-Free are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

Legal Notice: Trend Micro licenses this product in accordance with terms and conditions set forth in the License Agreement inside the product package. If you wish to review the License Agreement prior to purchase, visit: http://www.trendmicro.com/license. If you (or the company you represent) do not agree to these terms and conditions, promptly return the product and package to your place of purchase for a full refund.