Hosted Email Security Integration with Microsoft Office 365

This document highlights the benefits of Hosted Email Security (HES) for Microsoft™ Office™ 365 customers and provides step-by-step instruction on integration.
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Benefits from Combining HES and Office 365</td>
<td>4</td>
</tr>
<tr>
<td>Understanding How Email Flows Works</td>
<td>5</td>
</tr>
<tr>
<td>Inbound Email Set Up</td>
<td>6</td>
</tr>
<tr>
<td>Outbound Email Set Up</td>
<td>18</td>
</tr>
</tbody>
</table>
INTRODUCTION

Office 365 is Microsoft’s cloud solution for accessing email, calendar, and Microsoft office tools. Office 365 allows organizations to host their entire email architecture at an off-site location, and it allows Microsoft to manage all the day-to-day aspects of your organization’s email.

Trend Micro has designed Hosted Email Security (HES) for customers who are using either cloud-based or onsite email.

Unlike traditional onsite email solutions where a simple cable could be moved in order to add a layer of protection, cloud-based solutions require a different approach. This document highlights the benefits of HES for Office 365 customers, as well as step-by-step instruction on integration. This integration guide assumes a functioning Office 365 deployment.
BENEFITS OF COMBINING HOSTED EMAIL SECURITY AND OFFICE 365

Moving your mail to the cloud does not mean you have to reduce your security. By integrating Trend Micro™ Hosted Email Security with Microsoft Office 365, you can now have the best of both worlds—true enterprise email security with the convenience of the cloud.

HES can provide the following features to enhance your Office 365 email security:

- **Layered protection**: Provides protection on phishing, spam, and graymail with multiple techniques, including sender reputation, content and image analysis, machine learning, and more.
- **Email fraud protection**: Protects against Business Email Compromise (BEC) with enhanced machine learning, combined with expert rules, analyzing both the header and content of the email.
- **Cloud sandboxing**: Includes cloud sandboxing for automatic in-depth simulation and analysis of potentially malicious attachments in a secure virtual environment hosted by Trend Micro. Cloud sandbox leverages proven Trend Micro™ Deep Discovery™ sandboxing technology, which has achieved a “Recommended” rating by NSS Labs.

Adding HES on top of Microsoft Office 365 offers enhanced security, especially with spear-phishing and targeted attack protection, providing you with an additional layer of security against advanced malware and zero-day exploits.
UNDERSTANDING HOW EMAIL FLOW WORKS

In order to better understand how HES works in conjunction with Microsoft Office 365, the path the email message takes must first be understood.

1. An email is initiated from one organization to the other. Let’s say an email from someone at Trend Micro to someone at Example.com is sent.

2. The Trend Micro mail server will look up the MX record of Example.com. This record will contain the Domain Name or IP address of the first hop in Example.com’s email architecture. This first hop is the first level of inspection that Example.com wants performed on their email.

3. Since Example.com is using Trend Micro HES, this will be the first hop for the inbound email.

4. HES then inspects the email via Trend Micro’s world class email and web reputation service for threats such as:
   a. Spam
   b. Phishing
   c. Viruses
   d. Spyware
5. If the email passes the HES checks, it is then sent to Example.com’s next hop, which is their Microsoft Office 365 cloud email server.

6. After further processing by Microsoft Office 365, the email is then sent to the recipient’s mailbox.

INBOUND EMAIL SET UP

Configuring your Hosted Email Security Settings

1. Configure the corresponding inbound settings in Trend Micro HES to route emails sent to your domain to Office 365.
   a. Log into the HES main page
   b. From the above column click on the following:
      i. Domains
      ii. Add
   c. For the domain that is being routed:
      i. Input the IP address or host name of your Office 365 Server in the “Inbound Servers” field. This can either be found by performing an nslookup or through the user interface in Microsoft Office 365.
      ii. Input the Port for your Office 365 server. (Normally, it’s port 25)
      iii. Input the preference for your server (sometimes referred to as distance, is a value from 1 to 100.)
   d. Click “Add Domain” to save your setting.
DNS records
The following DNS records must be configured at your DNS hosting provider. The records that you configure depend on the domain purpose that you set.

Need help adding these records? See step-by-step instructions for creating DNS records at popular DNS hosting providers.

Exchange Online

<table>
<thead>
<tr>
<th>TYPE</th>
<th>PRIORITY</th>
<th>HOST NAME</th>
<th>POINTS TO ADDRESS</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX</td>
<td>0</td>
<td>@</td>
<td>trendenablement.com.mail.protection.outlook.com</td>
<td>1 Hour</td>
</tr>
<tr>
<td>CNAME</td>
<td>-</td>
<td>autodiscover</td>
<td>autodiscover.outlook.com</td>
<td>1 Hour</td>
</tr>
</tbody>
</table>

Configuring Microsoft Office 365 Settings

1. Log into your Microsoft Office 365 administrator center account
a. Click on **ADMIN** from navigation menu

b. Then **Exchange** under **Admin centers**

c. Then **mail flow** from left navigation

d. Then **connectors** from top navigation menu
2. Add an Inbound Connector.
3. Connectors are where you will add the information about the inbound HES server.
   
   a. Be sure to define the Connector name and the domains you want to accept.
4. In the **Name** field, enter a descriptive name for the inbound connector.
5. Choose: **Use the sender’s IP address**

![New Connector - Mozilla Firefox](https://i.imgur.com/2.png)

6. In **Specify the sender IP addresses range** field, enter the IP address or addresses for the organization you want to add to the safe list. This will be the IP address of the HES Server. This information is available in the welcome email (not the license registration email) or available in this support article: [http://esupport.trendmicro.com/solution/en-us/1055066.aspx](http://esupport.trendmicro.com/solution/en-us/1055066.aspx).

**NOTE:** You may have Office 365 only accepts rr in range of 24 to 32 (nnn.nnn.nnn.nnn/rr), please modify the rr from HES instructions to the closest Office 365 allows you to set. For example: 216.104.0.0/19 you can enter as 216.104.0.0/24.

The IP addresses in the screenshots above may be subject to change without notice, **always use information from the welcome email or support article as primary source.**
7. Choose the security restrictions you want:
8. Click save.

Point the MX record of your domain to Trend Micro HES

**Important! This step should be performed last to guarantee mail flow.**

The MX record or Mail Exchange record is the IP address or domain name that will be receiving your mail. This has to be the first destination of the email. In this case, it must be the public IP address of the HES server. This address must be configured through your ISP or domain registrar:

1. Lower the TTL of the MX record to help increase delivery reliability
2. Migrate MX record to new HES IP address
**Add an email flow rule to bypass spam filtering**

Turn off spam filtering in Exchange Online and use Hosted Email Security only

1. Log into your Microsoft Office 365.

2. Go to Exchange admin center page (select Admin centers | Exchange from title bar).

3. Click mail flow from left navigation, select rules.

4. Select “Bypass spam filtering” from pull-down menu.

5. In the Rule window, complete the required fields.
   a. Name: Turn off spam filter in Office 365.
   b. Apply this rule if
      i. Select The sender… | IP address is in any of these ranges or exactly matches.
      ii. In the Specify IP address ranges window, enter the same IP addresses from step 6 of INBOUND MAIL SETUP section above.
      iii. Click the add icon for each range.
      iv. Click ok.
   c. Do the following: Set the spam confidence level (SCL) to... - Bypass spam filtering
   d. Except if: Do not add an exception
   e. Audit this rule with severity level: Not specified
   f. Choose a mode for this rule: Enforce

6. Click Save.

**Add an email flow rule to lock down Exchange Online**

This accepts only emails from Hosted Email Security to ensure spammers cannot bypass.

1. Log into your Microsoft Office 365.

2. Go to Exchange admin center page (select Admin centers | Exchange from title bar).
3. Click **mail flow** from left navigation, select **rules**.

4. Select “**Restrict messages by sender or recipient ...**” from pull-down menu.
   a. Name: “Only accept inbound mail from HES”
   b. **Apply this rule if**
      i. Select **The sender is located**.
      ii. In the select **sender location** window, select **Outside the organization**
      iii. Click **ok**
   c. **Do the following**: **Delete the message without notifying anyone**
   d. **Audit this rule with severity level**: **Not specified**
   e. **Choose a mode for this rule**: **Enforce**

5. In the **Rule** window, complete the required fields.

6. **Add an exception to the allow email flow from Hosted Email Security**
   a. Click **More options**
   b. **Under Except if, click add exception**
   c. Select **The sender... | IP address is in any of these ranges or exactly matches.**
   d. In the **Specify IP address ranges** window, enter the same IP addresses from step 6 of INBOUND EMAIL SETUP section above.
   e. Click the add icon for each range
   f. Click **ok**

7. Click **save**.

**Disable SPF hard fail check**

This accepts the emails from Hosted Email Security, which may fail SPF check.

1. Log into your Microsoft Office 365.

2. Go to Exchange admin center page (select **Admin centers** | **Exchange** from title bar).
3. Click **protection** from left navigation, select **spam filter**.

4. Change the advanced options of your spam policy
   a. Click the spam policy to open it
   b. Choose **advanced options** from the left navigation
   c. Find **SPF record: hard fail** and choose **Off** for this option

   ![Image of advanced options setting]({image_url})

   - **Default**
     - Specify whether to mark messages that include these properties as spam.
     - **Empty messages:**
       - **Off**
     - **JavaScript or VBScript in HTML:**
       - **Off**
     - **Frame or Iframe tags in HTML:**
       - **Off**
     - **Object tags in HTML:**
       - **Off**
     - **Embed tags in HTML:**
       - **Off**
     - **Form tags in HTML:**
       - **Off**
     - **Web bugs in HTML:**
       - **Off**
     - **Apply sensitive word list:**
       - **Off**
   - **SPF record: hard fail:**
     - **Off**
   - **Conditional Sender ID filtering: hard fail:**
     - **Off**
   - **NDR backscatter:**
     - **Off**

   d. Click **Save** for this setting
OUTBOUND EMAIL SET UP

Configure your Hosted Email Security Settings

1. Configure the corresponding outbound settings in Trend Micro HES to route emails sent from your domain from Office 365.
   a. Log into the HES main page
      b. From the above column click on the following:
         i. Domains
         ii. Special domain name
      c. Check the checkbox for **Enable outbound protection**
      d. Select checkbox button for **Office 365**
      e. Click **Save**

Configure Microsoft Office 365 Settings

1. Log into your Microsoft Office 365 administrator center account
   a. Click on **ADMIN** from navigation menu
   b. Then **Exchange** under **Admin centers**
   c. Then mail flow from left navigation
   d. Then connectors from top navigation menu
2. Add an Outbound Connector as follows:
3. Name your connector and add description.

![Image of New Connector setup screen]

- Name: Trend Micro HES outbound
- Description:
- Turn it on
4. Choose the way you want to use this connector.
5. Add HES Relay FQDN to: **Route email through these smart hosts**

- Add the fully qualified domain name (FQDN) for the purpose of relay messages to this Hosted Email Security MTA. This FQDN is located in the welcome email (sent to the administrator after you have completed Hosted Email Security activation process). ([http://docs.trendmicro.com/en-us/enterprise/hosted-email-security-administrator-guide/about-domain-management/configuring-a-domain.aspx](http://docs.trendmicro.com/en-us/enterprise/hosted-email-security-administrator-guide/about-domain-management/configuring-a-domain.aspx))
6. Choose the way to connect to HES.
7. Review your setting.
8. Add one test email to verify this connector.
9. Validate this email address and save the connector.

Note: when you have more than one domains in your Office 365 system, the validation may not succeed for “Send test email” part. Sometimes, it’s because that the default domain is not the one you register to HES. Choose the domain which you register to HES and enable outbound filter and make it as default domain like below:
After that, try to set your collector again.

10. Click **save**.
Add an email flow rule to use the HES Outbound connector

1. Log into your Microsoft Office 365.
2. Go to Exchange admin center page (select Admin centers | Exchange from title bar).
3. Click mail flow from left navigation, select rules.
4. Click “+” sign and “create a new rule”

   a. Complete the following fields:

      i. Name: HES Outbound

      ii. Apply this rule if:

         1. Select “The recipient is located”, a new pop out console will show.

         2. Select “Outside the organization” click ok.

         3. Click “More Options” to show more conditions.

Choose a mode for this rule:
- Enforce
- Test with Policy Tips
- Test without Policy Tips

Rights Management Services (RMS) is a premium feature
iii. Do the following:

1. In the dropdown menu, mouse over to “Redirect message to” and then select “the following connector.”

2. Select the outbound connector you created for HES.

iv. Choose Mode:

1. Select “Enforce”

v. Click save

Congratulations! You have completed the installation process. Office 365 is now secured by Trend Micro Hosted Email Security.