A Trend Micro Integration Guide I **Aug 2018**

Trend Micro™ Email Security Integration with Microsoft Office 365

» This document highlights the benefits of Trend Micro™ Email Security (TMEMS) for Microsoft™ Office™ 365 customers and provides step-by-step instruction on integration.

TABLE OF CONTENTS

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 Trend Micro™ Email Security (TMEMS) 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 TMEMS 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 TREND MICRO™ EMAIL SECURITY AND OFFICE 365

Moving your mail to the cloud does not mean you have to reduce your security. By integrating Trend Micro™ 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.

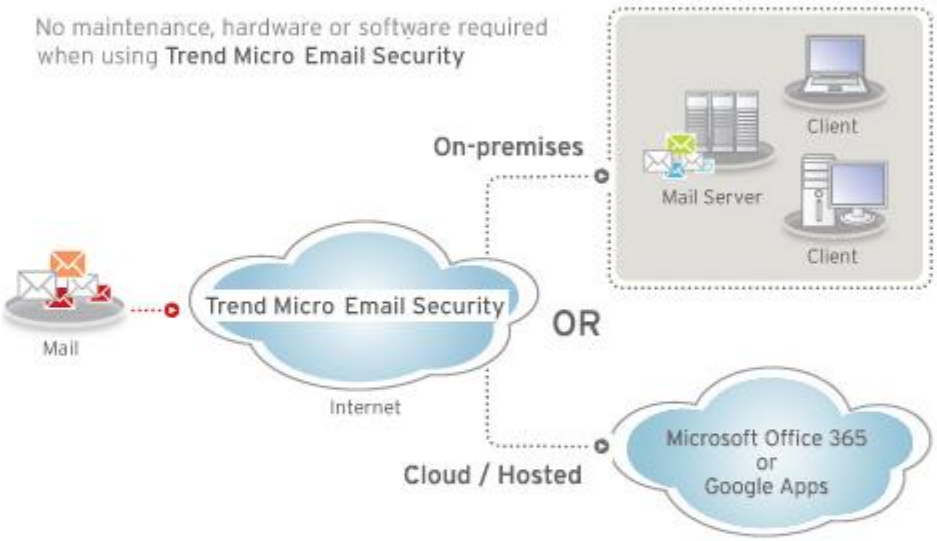
TMEMS can provide the following features to enhance your Office 365 email security:

- **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 TMEMS 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 TMEMS works in conjunction with Microsoft Office 365, the path the email message takes must first be understood.


No maintenance, hardware or software required when using Trend Micro Email Security
On-premises
Client
Mail Server
Client
Mail
Trend Micro Email Security
Internet
OR
Cloud / Hosted
Microsoft Office 365
or
Google Apps

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 Email Security, this will be the first hop for the inbound email.

4. TMEMS 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

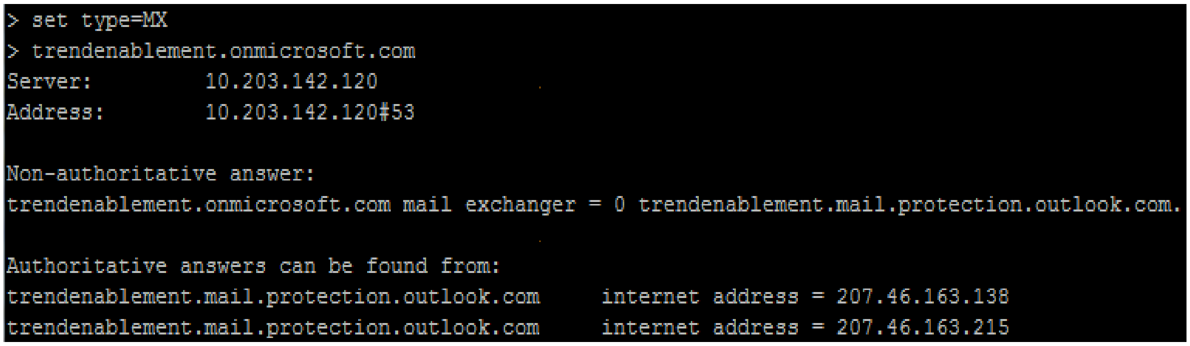
5. If the email passes the TMEMS checks, it is then sent to Example.com's next hop, which is their Microsoft Office 365 cloud email server.

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

INBOUND EMAIL SET UP

Configuring your Trend Micro Email Security Settings

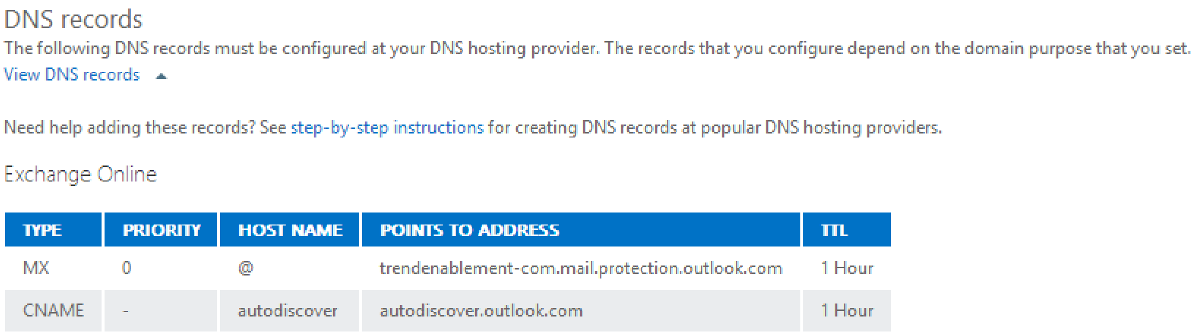
1. Configure the corresponding inbound settings in Trend Micro Email Security to route emails sent to your domain to Office 365.
   a. Log into the TMEMS main page
   b. From the above column click on the following:
      i. **Domains**
      ii. **Add**
   c. For the domain that is being routed:
      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.
      Note: Microsoft generates MX records for your domains when you set them up in Exchange Online.
      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.



```
> set type=MX
> trendenablement.onmicrosoft.com
Server:         10.203.142.120
Address:        10.203.142.120#53

Non-authoritative answer:
trendenablement.onmicrosoft.com mail exchanger = 0 trendenablement.mail.protection.outlook.com.

Authoritative answers can be found from:
trendenablement.mail.protection.outlook.com     internet address = 207.46.163.138
trendenablement.mail.protection.outlook.com     internet address = 207.46.163.215
```



DNS records

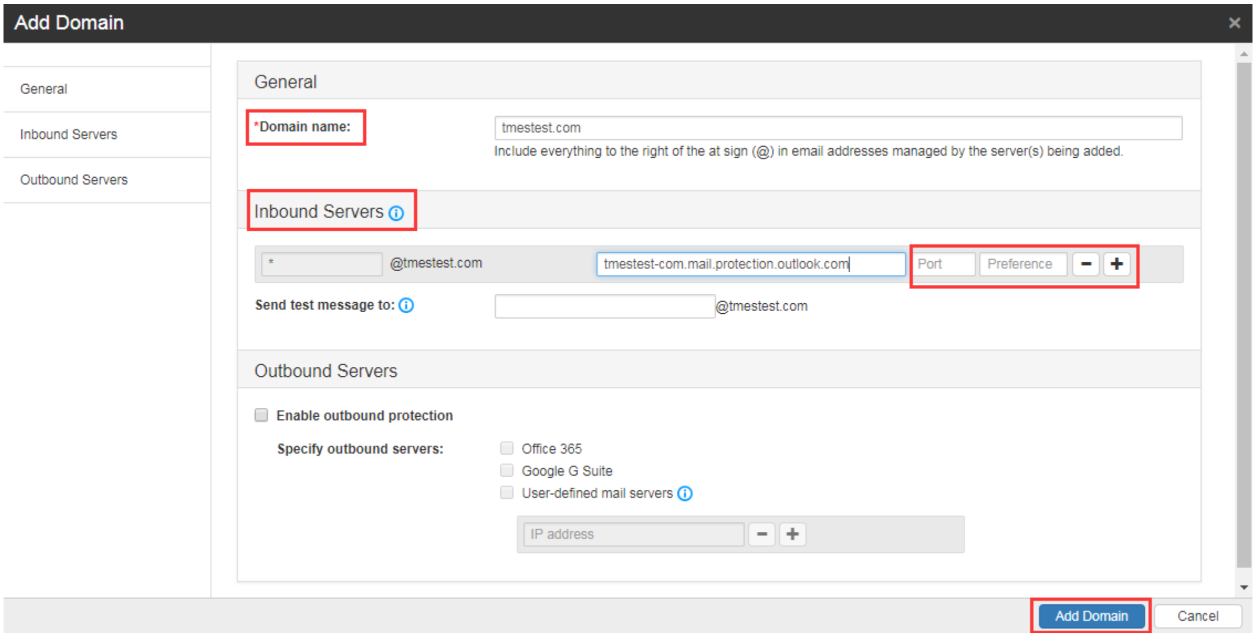
The following DNS records must be configured at your DNS hosting provider. The records that you configure depend on the domain purpose that you set.

View DNS records ▲

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

Exchange Online

TYPE	PRIORITY	HOST NAME	POINTS TO ADDRESS	TTL
MX	0	@	trendenablement-com.mail.protection.outlook.com	1 Hour
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour



General

*Domain name: tmestest.com

Include everything to the right of the at sign (@) in email addresses managed by the server(s) being added.

Inbound Servers ⓘ

* @tmestest.com tmestest-com.mail.protection.outlook.com Port Preference − +

Send test message to: ⓘ @tmestest.com

Outbound Servers

□ Enable outbound protection

Specify outbound servers:

□ Office 365

□ Google G Suite

□ User-defined mail servers ⓘ

IP address − +

Configuring Microsoft Office 365 Settings

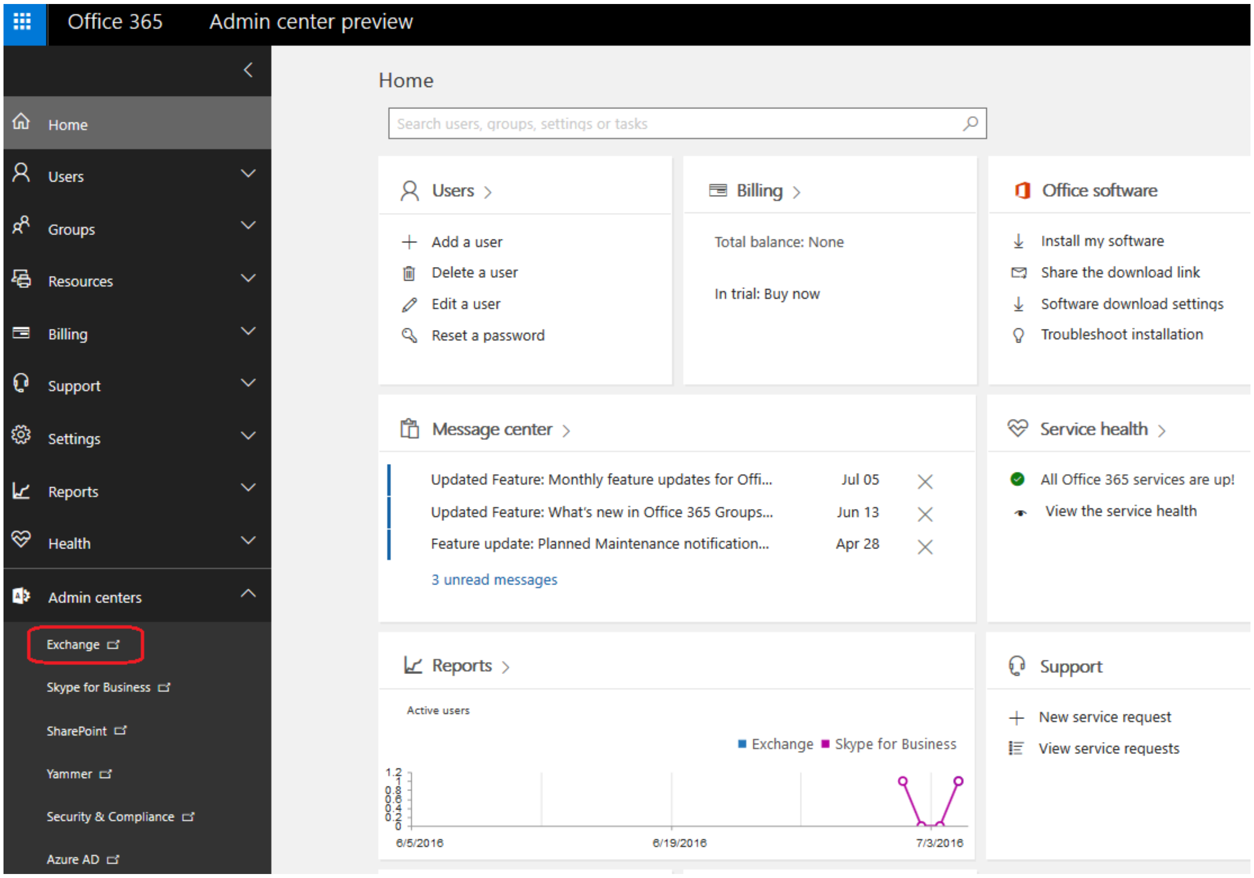
1. Log into your Microsoft Office 365 administrator center account

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



Total balance: None

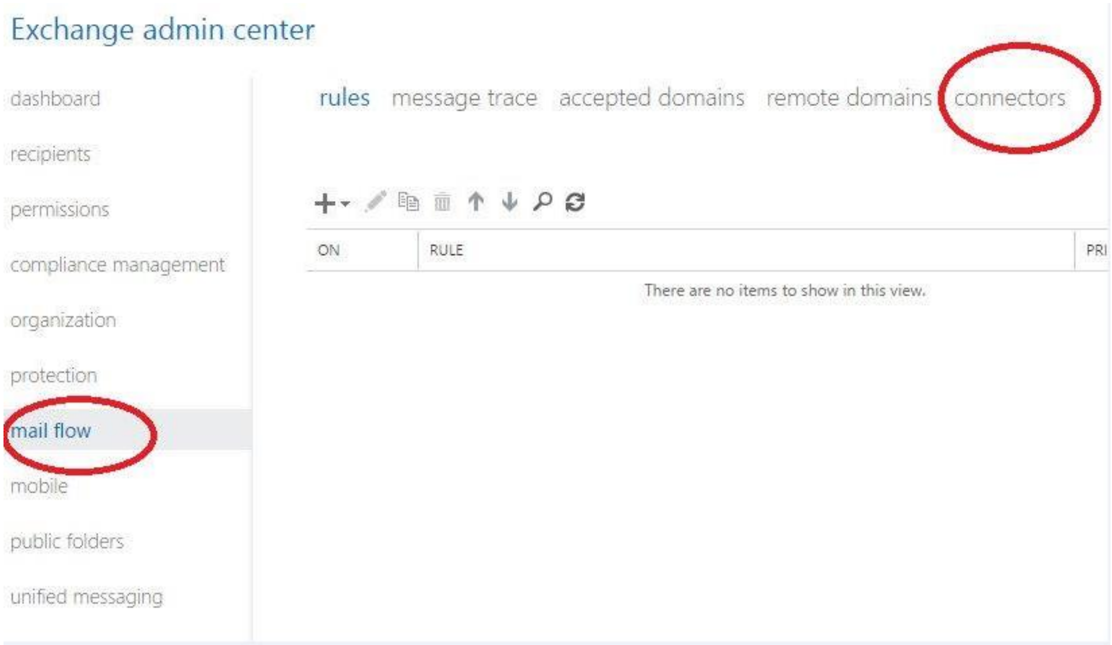
In trial: Buy now

Updated Feature: Monthly feature updates for Offi... Jul 05

Updated Feature: What's new in Office 365 Groups... Jun 13

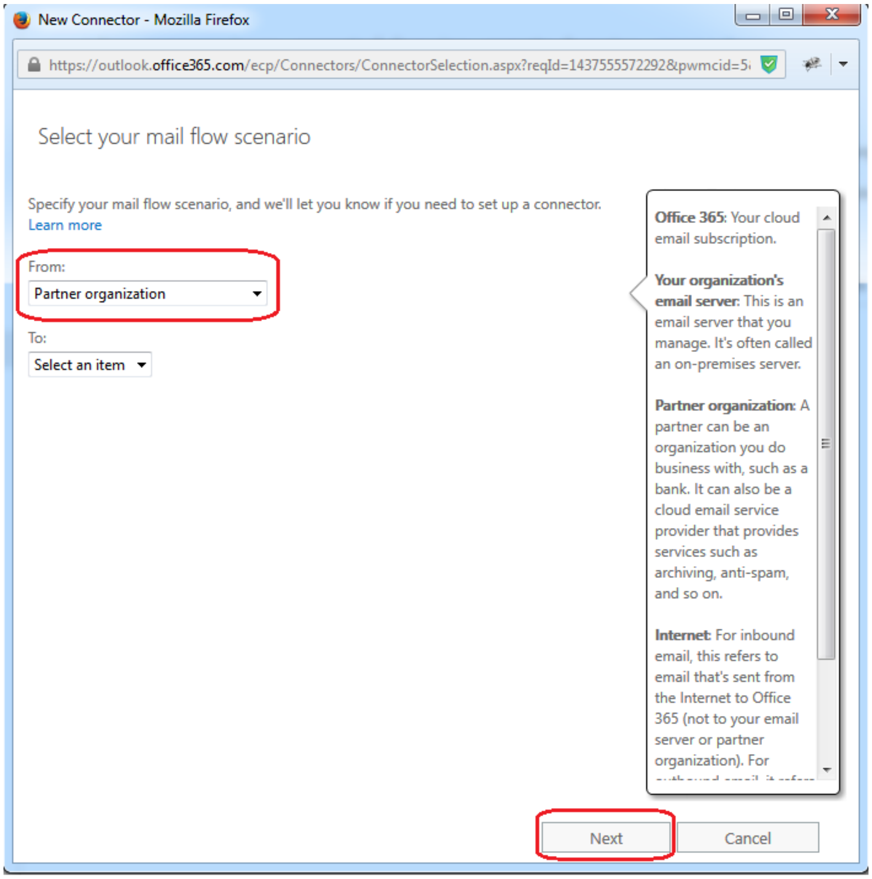
Feature update: Planned Maintenance notification... Apr 28

All Office 365 services are up!



There are no items to show in this view.

2. Add an Inbound Connector.


New Connector - Mozilla Firefox
https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?reqId=1437555572292&pwmcid=5
Next
Cancel

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. Learn more

From: Partner organization

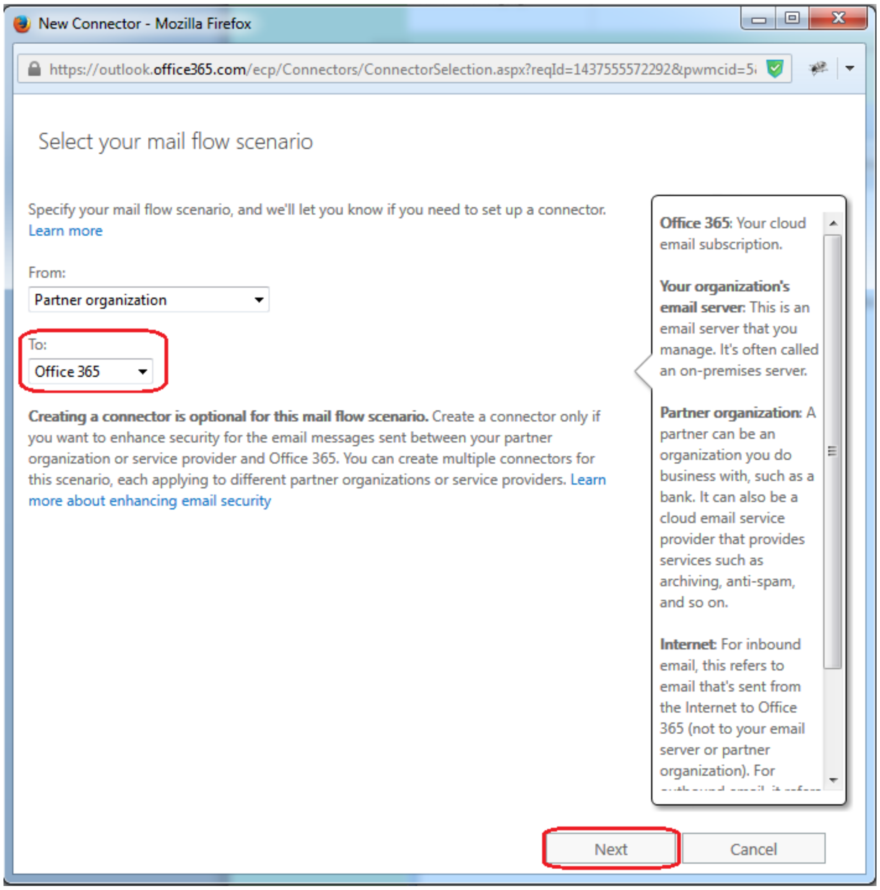
To: Select an item

Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

Partner organization: A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For


New Connector - Mozilla Firefox
https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?reqId=1437555722928&pwmcid=5

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. Learn more

From: Partner organization

To: Office 365

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between your partner organization or service provider and Office 365. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. Learn more about enhancing email security

Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

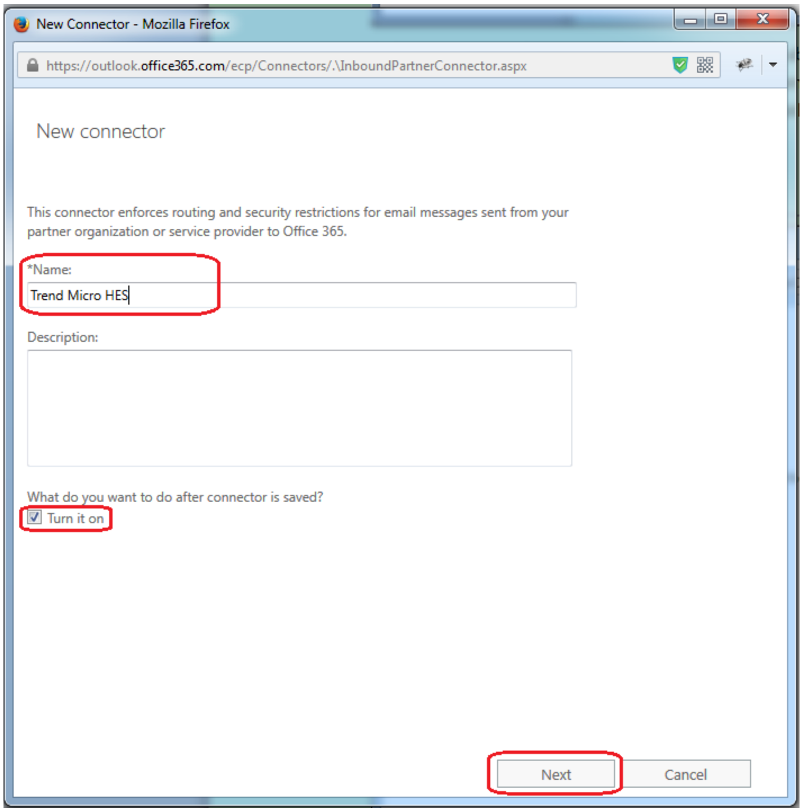
Partner organization: A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For

3. Connectors are where you will add the information about the inbound TMEMS 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.



New Connector - Mozilla Firefox
https://outlook.office365.com/ecp/Connectors/.\InboundPartnerConnector.aspx

New connector

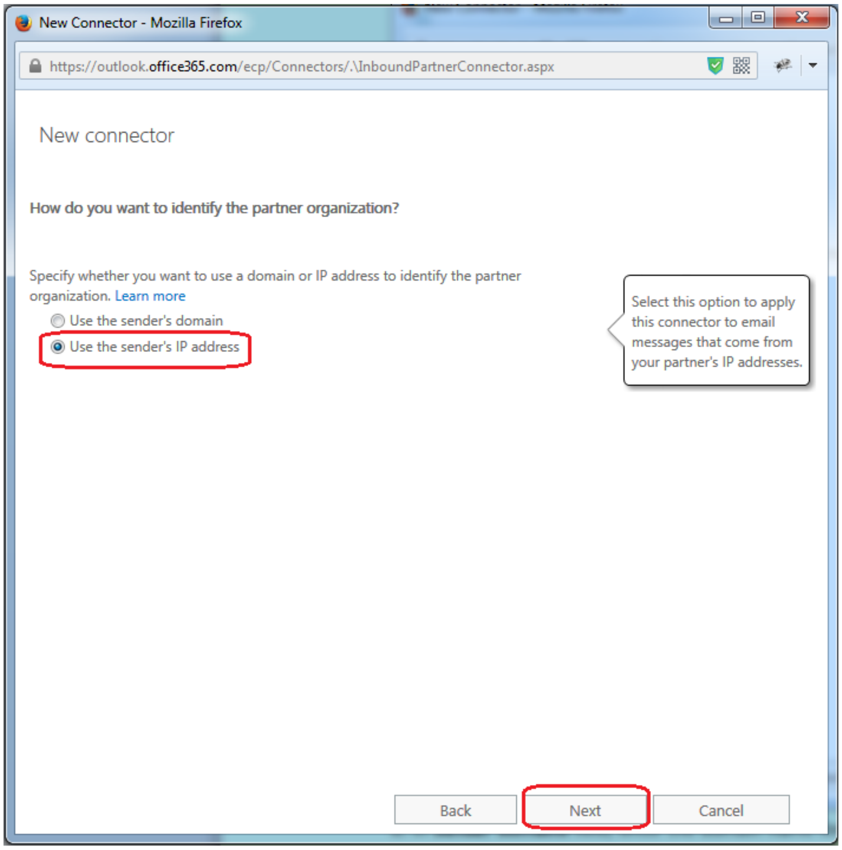
This connector enforces routing and security restrictions for email messages sent from your partner organization or service provider to Office 365.

*Name:
Trend Micro HES

Description:

What do you want to do after connector is saved?
☑ Turn it on

5. Choose: **Use the sender's IP address**



New Connector - Mozilla Firefox
https://outlook.office365.com/ecp/Connectors/.\InboundPartnerConnector.aspx

New connector

How do you want to identify the partner organization?

Specify whether you want to use a domain or IP address to identify the partner organization. Learn more

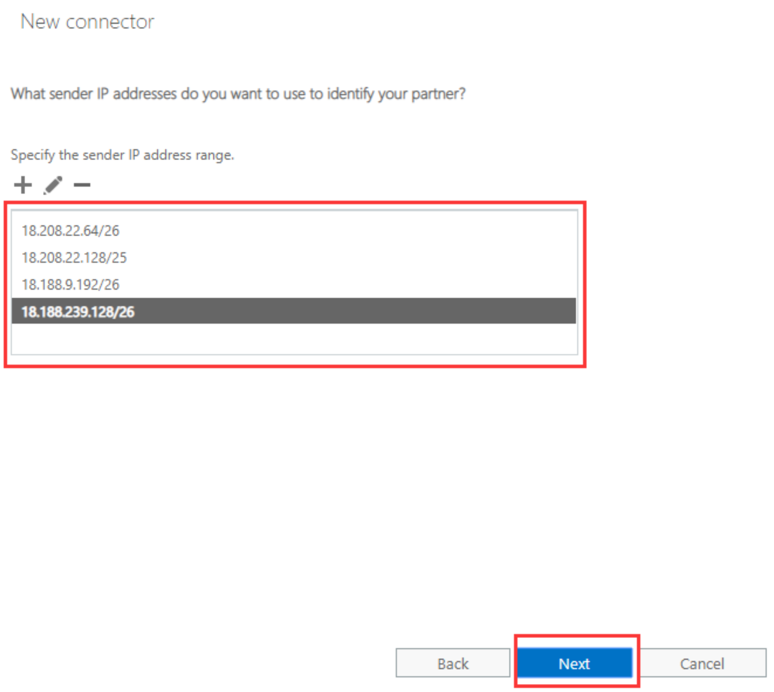
○ Use the sender's domain

● Use the sender's IP address

Select this option to apply this connector to email messages that come from your partner's IP addresses.

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 TMEMS 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~~.

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.***



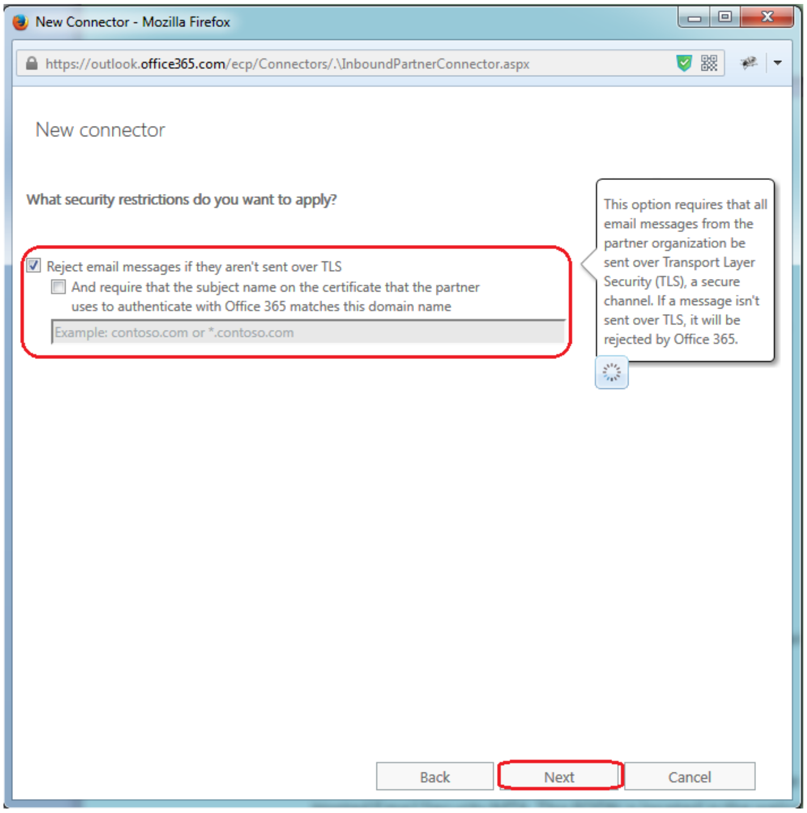
New connector

What sender IP addresses do you want to use to identify your partner?

Specify the sender IP address range.

18.208.22.64/26
18.208.22.128/25
18.188.9.192/26
18.188.239.128/26

7. Choose the security restrictions you want:



New Connector - Mozilla Firefox

https://outlook.office365.com/ecp/Connectors/.\InboundPartnerConnector.aspx

New connector

What security restrictions do you want to apply?

☑ Reject email messages if they aren't sent over TLS

□ And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or *.contoso.com

This option requires that all email messages from the partner organization be sent over Transport Layer Security (TLS), a secure channel. If a message isn't sent over TLS, it will be rejected by Office 365.

8. Click **save**

Point the MX record of your domain to Trend Micro Email Security

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 FQDN address of the TMEMS 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 TMEMS FQDN address

Add an email flow rule to bypass spam filtering

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

1. Log into your Microsoft Office 365.
2. Go to Exchange admin center page (select **Admin center**| **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 Trend Micro Email Security to ensure spammers cannot bypass.

1. Log into your Microsoft Office 365.
2. Go to Exchange admin center page (select **Admin center** | **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 TMEMS"
   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 Trend Micro 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.**

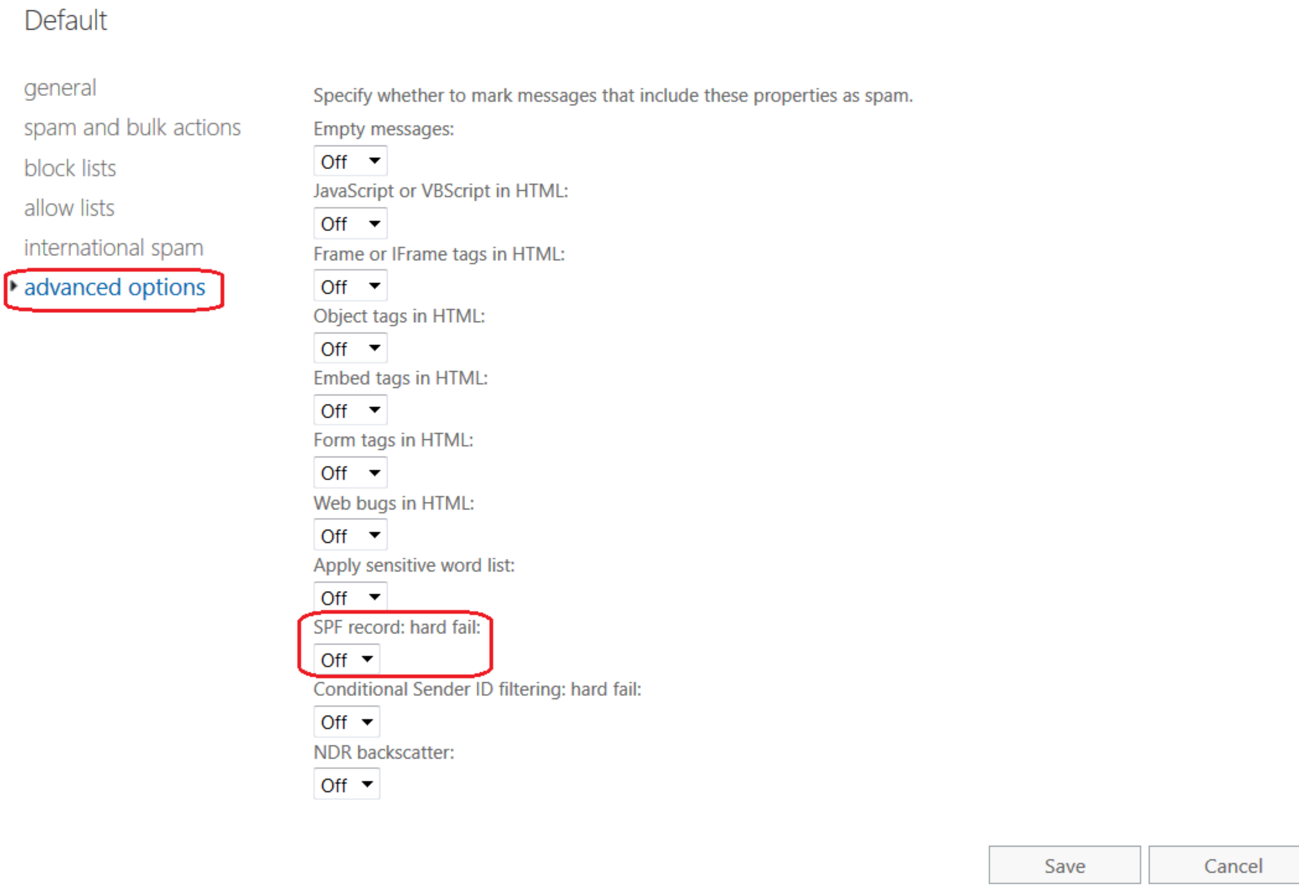
Disable SPF hard fail check

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

1. Log into your Microsoft Office 365.
2. Go to Exchange admin center page (select **Admin center**| **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



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 Trend Micro Email Security Settings

1. Configure the corresponding outbound settings in Trend Micro Email Security to route emails sent from your domain from Office 365.
   a. Log into the TMEMS 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

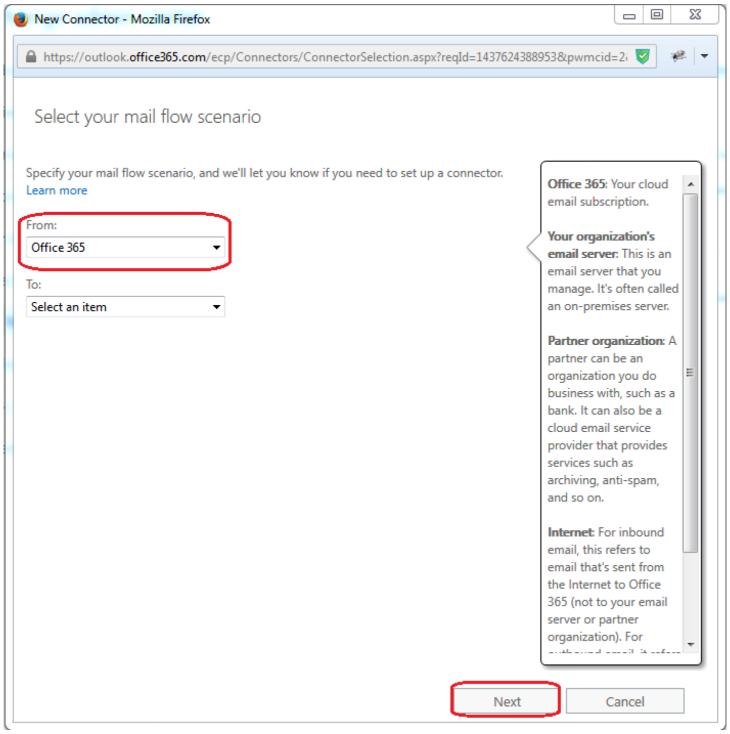
1. Log into your Microsoft Office 365 administrator center account
   a. Click on **ADMIN** from navigation menu

   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:


New Connector - Mozilla Firefox

https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?reqId=1437624388953&pwmcid=2

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
Learn more

From:
Office 365

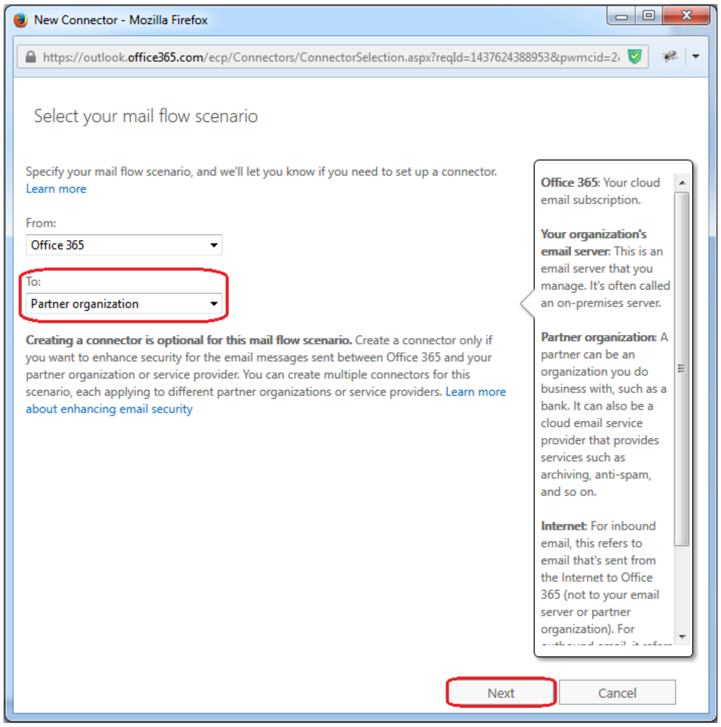
To:
Select an item

Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

Partner organization: A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For


New Connector - Mozilla Firefox

https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?reqId=1437624388953&pwmcid=2

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
Learn more

From:
Office 365

To:
Partner organization

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. Learn more about enhancing email security

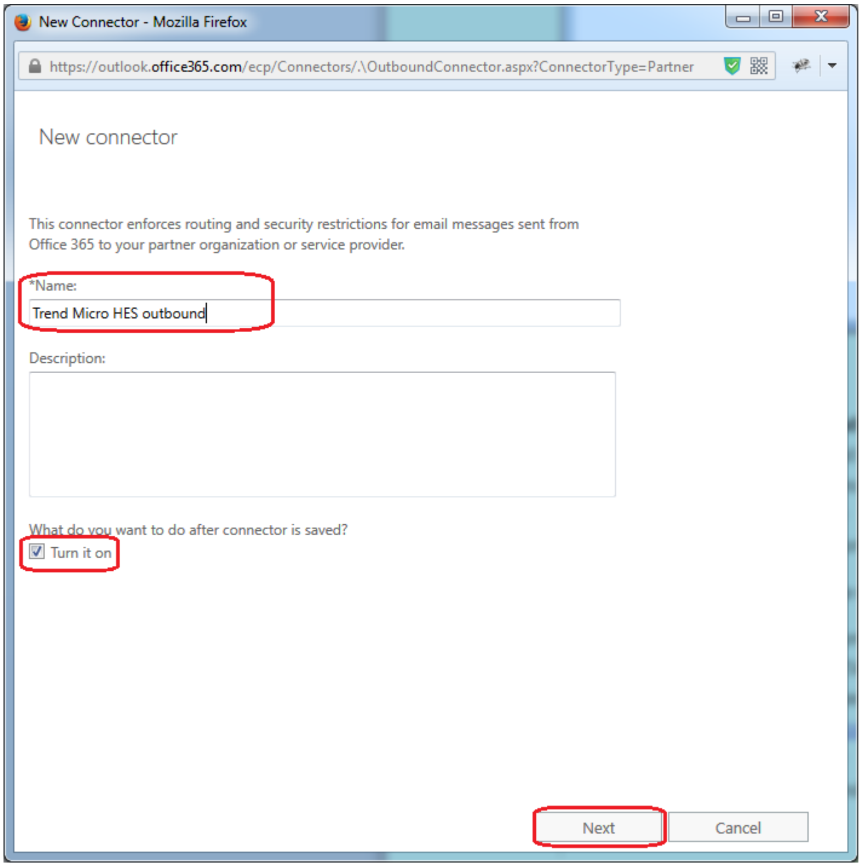
Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

Partner organization: A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For

3. Name your connector and add description.



New Connector - Mozilla Firefox

https://outlook.office365.com/ecp/Connectors/.\OutboundConnector.aspx?ConnectorType=Partner

New connector

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

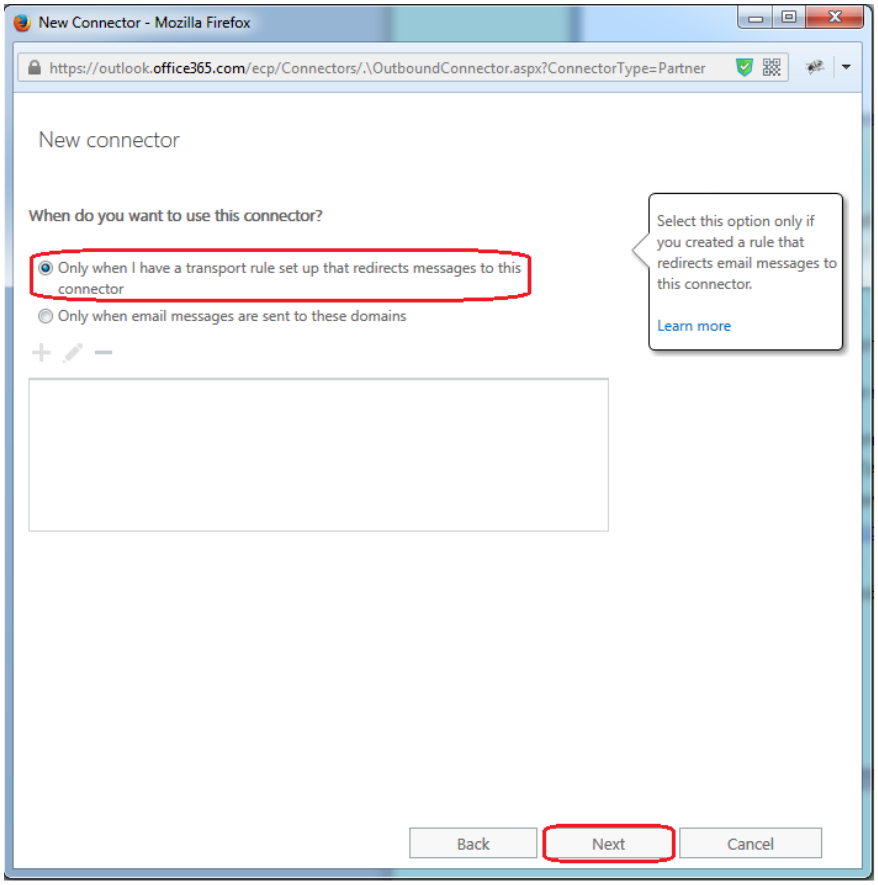
*Name:
Trend Micro HES outbound

Description:

What do you want to do after connector is saved?

☑ Turn it on

4. Choose the way you want to use this connector.



New Connector - Mozilla Firefox

https://outlook.office365.com/ecp/Connectors/.\OutboundConnector.aspx?ConnectorType=Partner

New connector

When do you want to use this connector?

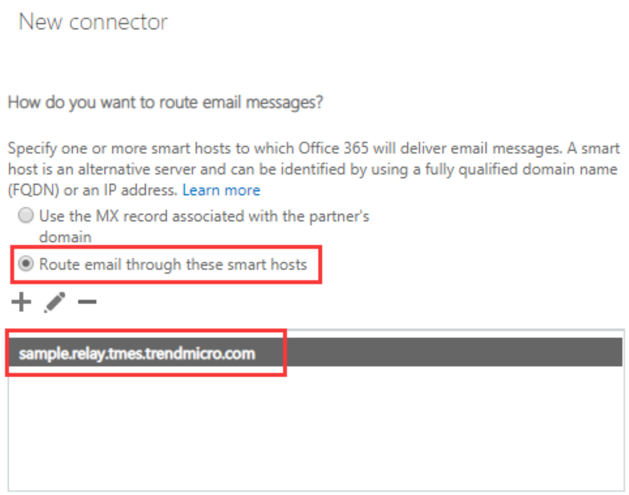
● Only when I have a transport rule set up that redirects messages to this connector

○ Only when email messages are sent to these domains

Select this option only if you created a rule that redirects email messages to this connector.

Learn more

5. Add TMEMS Relay FQDN to: **Route email through these smart hosts**



New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. Learn more

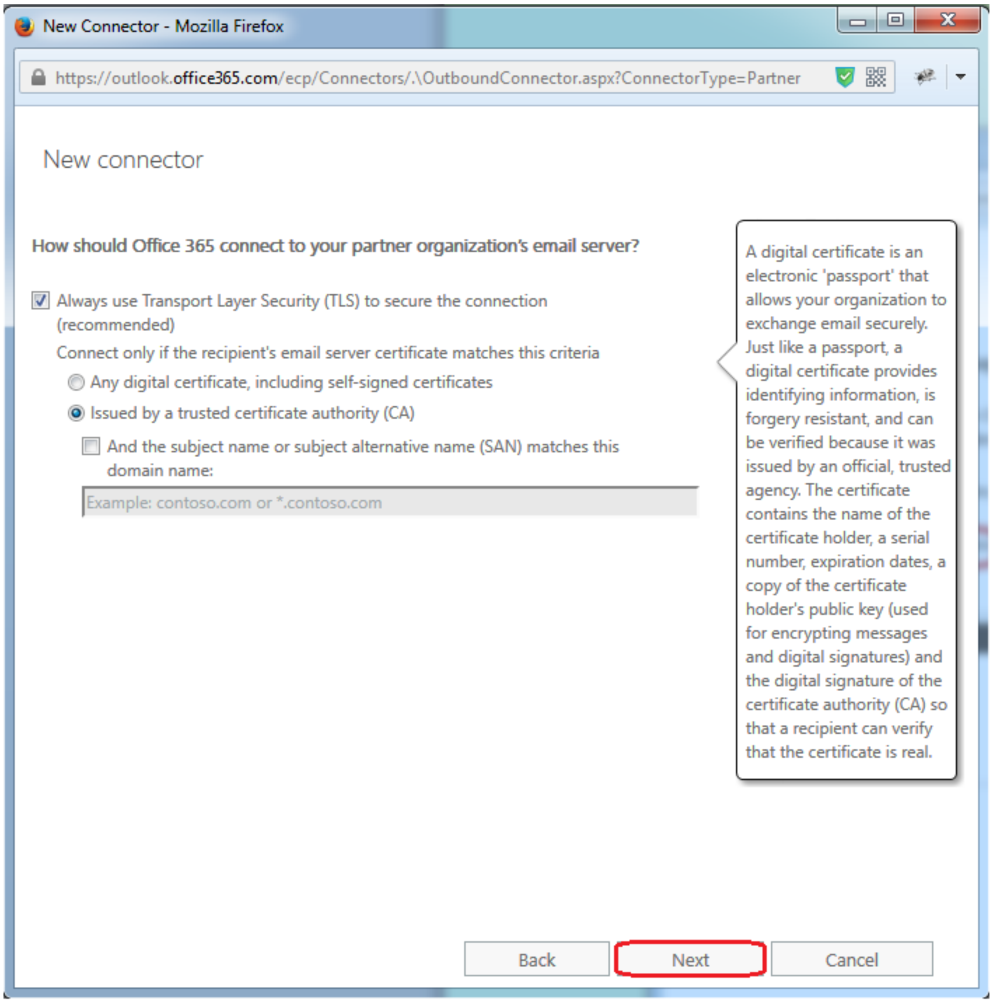
○ Use the MX record associated with the partner's domain

● Route email through these smart hosts

sample.relay.tmes.trendmicro.com

- Add the fully qualified domain name (FQDN) for the purpose of relay messages to this Trend Micro Email Security MTA. This FQDN is located in the welcome email (sent to the administrator after you have completed Trend Micro Email Security activation process). ~~(http://docs.trendmicro.com/all/smb/hes/vAll/en-us/olh/gsg/activating_service.html)~~

6. Choose the way to connect to TMEMS.



New Connector - Mozilla Firefox
https://outlook.office365.com/ecp/Connectors/.\OutboundConnector.aspx?ConnectorType=Partner

New connector

How should Office 365 connect to your partner organization's email server?

☑ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

○ Any digital certificate, including self-signed certificates

● Issued by a trusted certificate authority (CA)

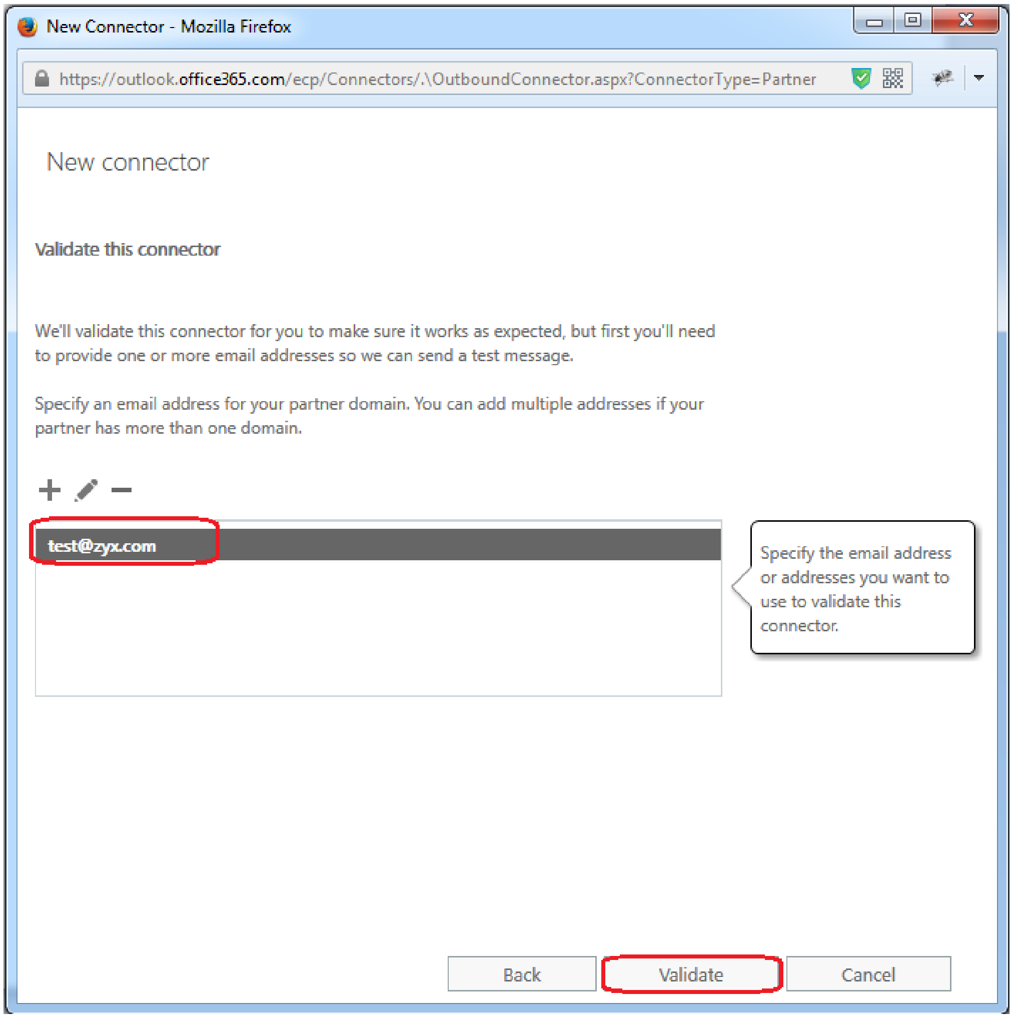
□ And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or *.contoso.com

A digital certificate is an electronic 'passport' that allows your organization to exchange email securely. Just like a passport, a digital certificate provides identifying information, is forgery resistant, and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate authority (CA) so that a recipient can verify that the certificate is real.

7. Review your setting.

8. Add one test email to verify this connector.



New Connector - Mozilla Firefox
https://outlook.office365.com/ecp/Connectors/.\OutboundConnector.aspx?ConnectorType=Partner

New connector

Validate this connector

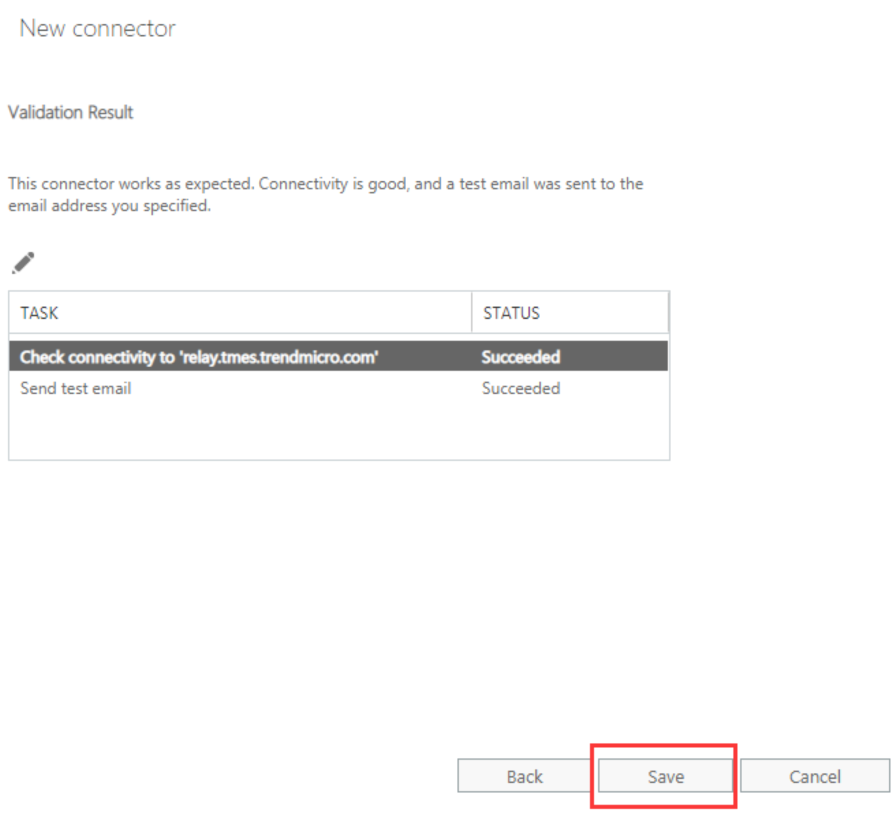
We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

Specify an email address for your partner domain. You can add multiple addresses if your partner has more than one domain.

test@zyx.com

Specify the email address or addresses you want to use to validate this connector.

9. Validate this email address and save the connector.



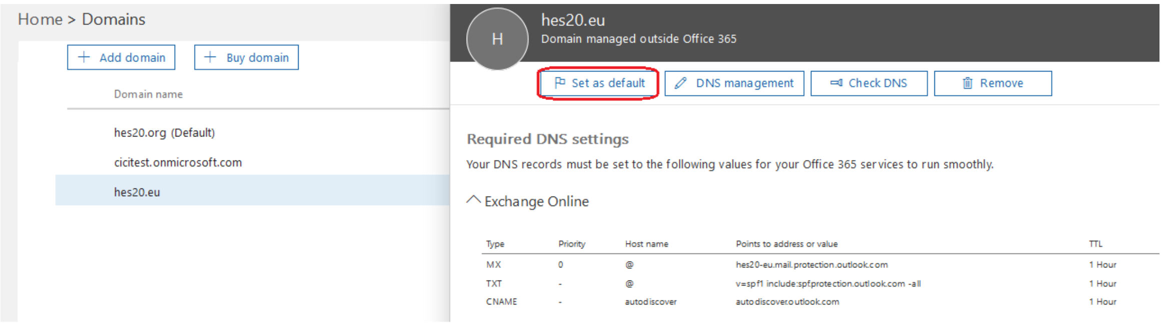
New connector

Validation Result

This connector works as expected. Connectivity is good, and a test email was sent to the email address you specified.

TASK	STATUS
Check connectivity to 'relay.tmes.trendmicro.com'	Succeeded
Send test email	Succeeded

Note: when you have more than one domains in your Office 365 system, the validation may not succeeded for "Send test email" part. Sometimes, it's because that the default domain is not the one you register to TMEMS. Choose the domain which you register to TMEMS and enable outbound filter and make it as default domain like below:



hes20.org (Default)
cicitest.onmicrosoft.com
hes20.eu

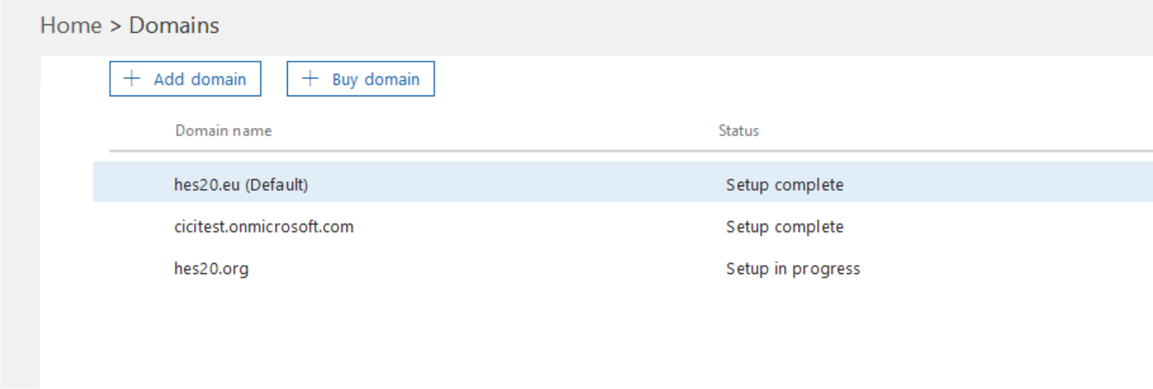
hes20.eu
Domain managed outside Office 365

Required DNS settings

Your DNS records must be set to the following values for your Office 365 services to run smoothly.

Exchange Online

Type	Priority	Host name	Points to address or value	TTL
MX	0	@	hes20-eu.mail.protection.outlook.com	1 Hour
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour



Home > Domains

Domain name	Status
hes20.eu (Default)	Setup complete
cicitest.onmicrosoft.com	Setup complete
hes20.org	Setup in progress

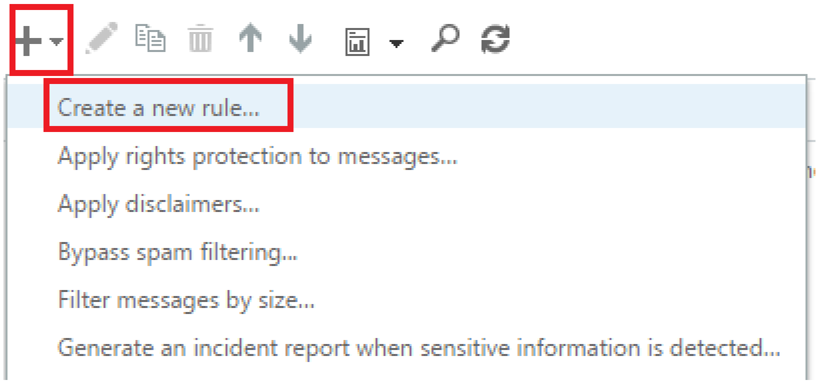
After that, try to set your collector again.

10. Click **save**.

Add an email flow rule to use the TMEMS 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**”


Create a new rule...
Apply rights protection to messages...
Apply disclaimers...
Bypass spam filtering...
Filter messages by size...
Generate an incident report when sensitive information is detected...

a. Complete the following fields:

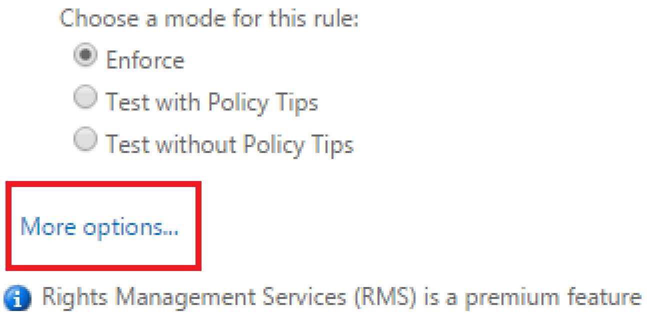
i. Name: TMEMS Outbound

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

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 TMEMS.

iv. Choose Mode:

1. Select "**Enforce**"

v. Click **save**

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

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1408.257.2003