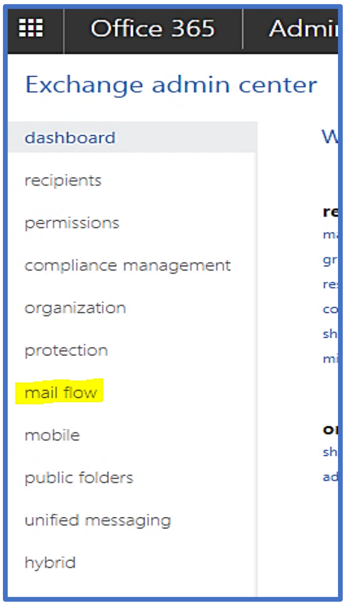
How to Configure the Outbound Smart Host for Office 365



Do This if your Organization hasn't updated their SPF for Office365:

Your organization should already have a SPF record for the domain(s) registered with Office 365. When implementing ExchangeDefender with Office 365, this record must be updated in the DNS zone for the relevant domain to include the following:

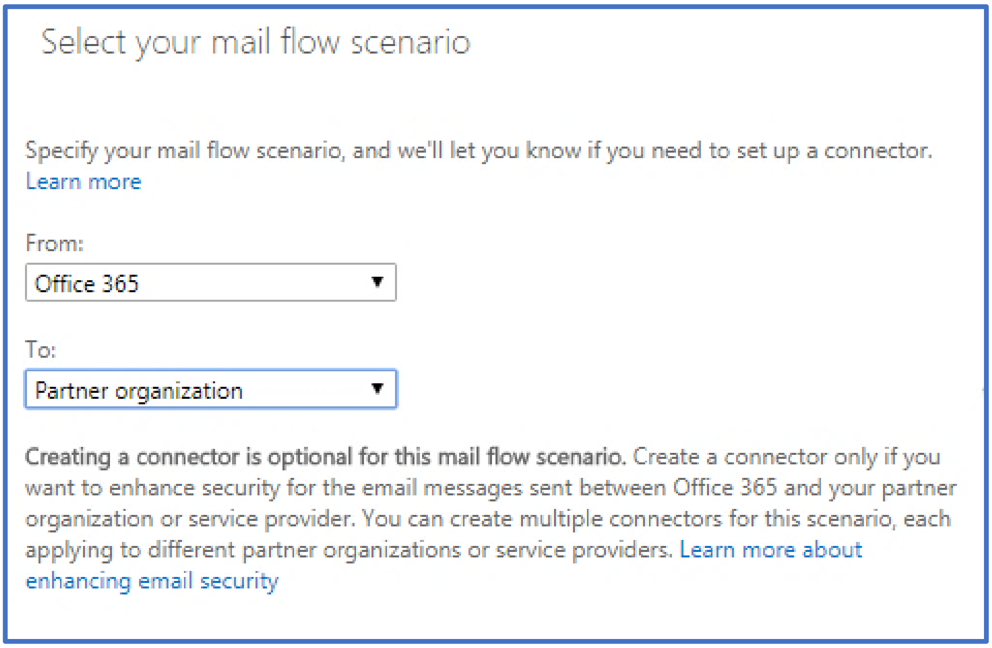
Remove: v=spf1 include:spf.protection.outlook.com –all
Replace with or add: v=spf1 include:exchangedefender.com ~all
Configuring Outbound Smarthost connector:

Log in to the Office 365 Administration Console.

Select the Admin | Exchange menu item. The Exchange Admin Center is displayed. Once displayed, in the menu on the left hand side, click '**mail flow**' as shown (right).

From here you're going to select '**connectors**'

From there you're going to click the '**+**' button and you'll be greeted with the following context menu:



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

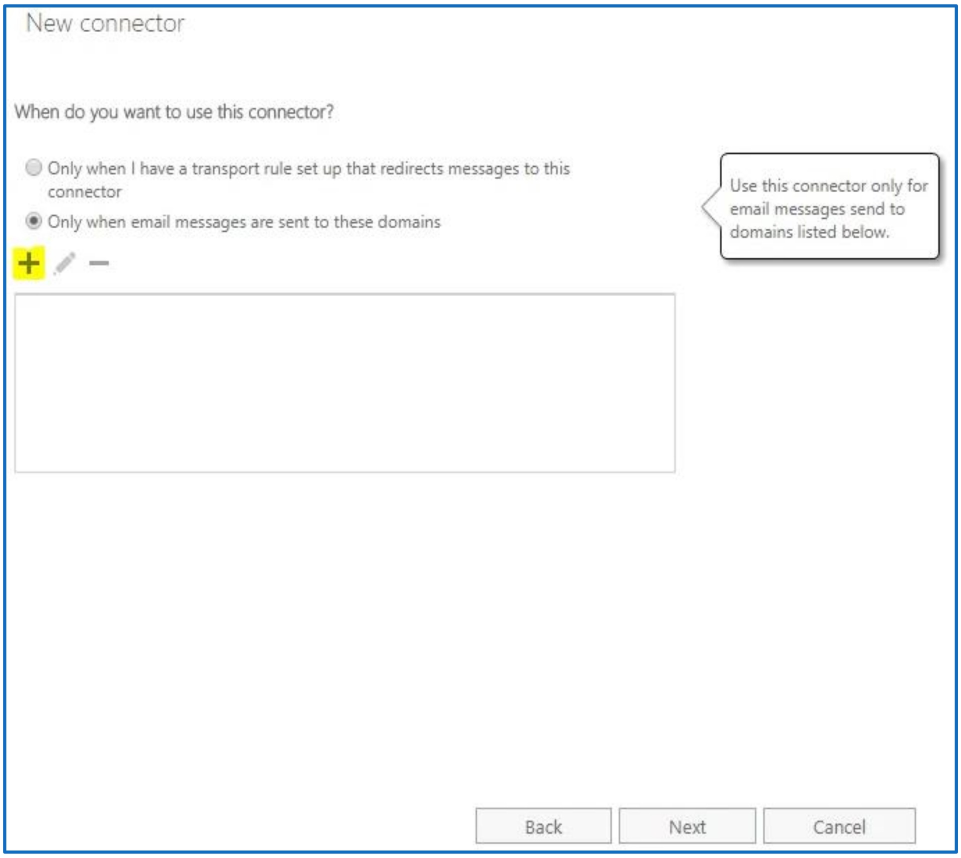
To: Partner organization

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

Once you've selected '**Office365**' and '**Partner Organization**' click the '**Next**' button

Enter the name of the connector (Can be a name of your choosing, we chose Exchange Defender for the purposes of this guide) After that, make sure the check box for '**Turn it on**' is selected then press '**Next**'

On this screen, select the option for **'Only when email messages are sent to these domains**' and click the '**+**' button to add the domains.



New connector

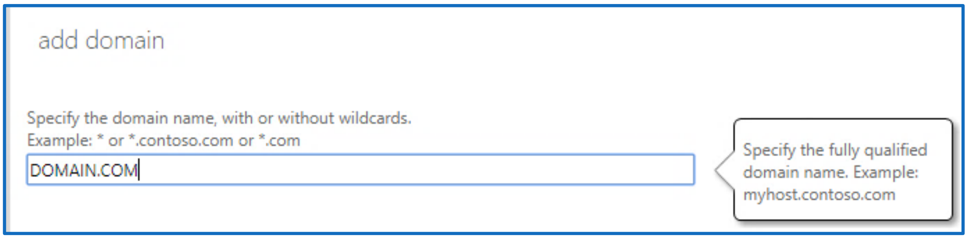
When do you want to use this connector?

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

● Only when email messages are sent to these domains

Use this connector only for email messages send to domains listed below.

Here you would **add the domain**, after you're done hit the **'Ok'** button.



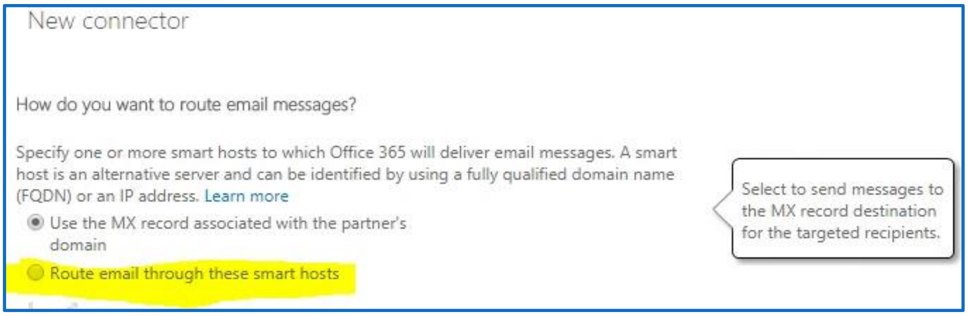
add domain

Specify the domain name, with or without wildcards.
Example: * or *.contoso.com or *.com

DOMAIN.COM

Specify the fully qualified domain name. Example: myhost.contoso.com

Next, you'll be asked how you would like to route the messages. Select the option that reads **'Route email through these smart hosts**' and then hit the '**+**' button



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

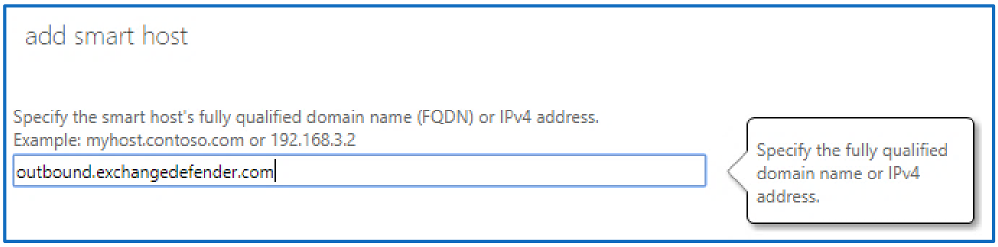
● Use the MX record associated with the partner's domain

○ Route email through these smart hosts

Select to send messages to the MX record destination for the targeted recipients.

From there you'll be asked to add a smart host.

Add'outbound.exchangedefender.com' as you see it in the screenshot (right).



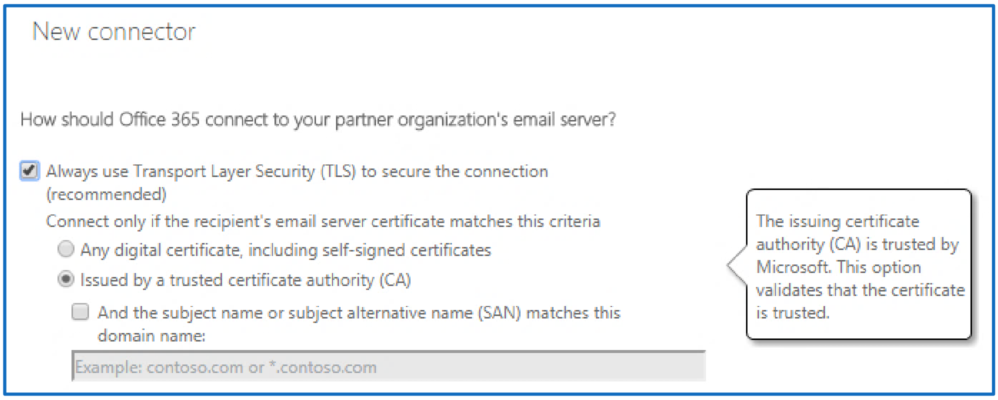
add smart host

Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.
Example: myhost.contoso.com or 192.168.3.2

outbound.exchangedefender.com

Specify the fully qualified domain name or IPv4 address.

Once you've entered the smarthost hit the '**Save**' button. From there you'll be taken to the TLS screen. **Keep all options default** as shown in the screenshot below.



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

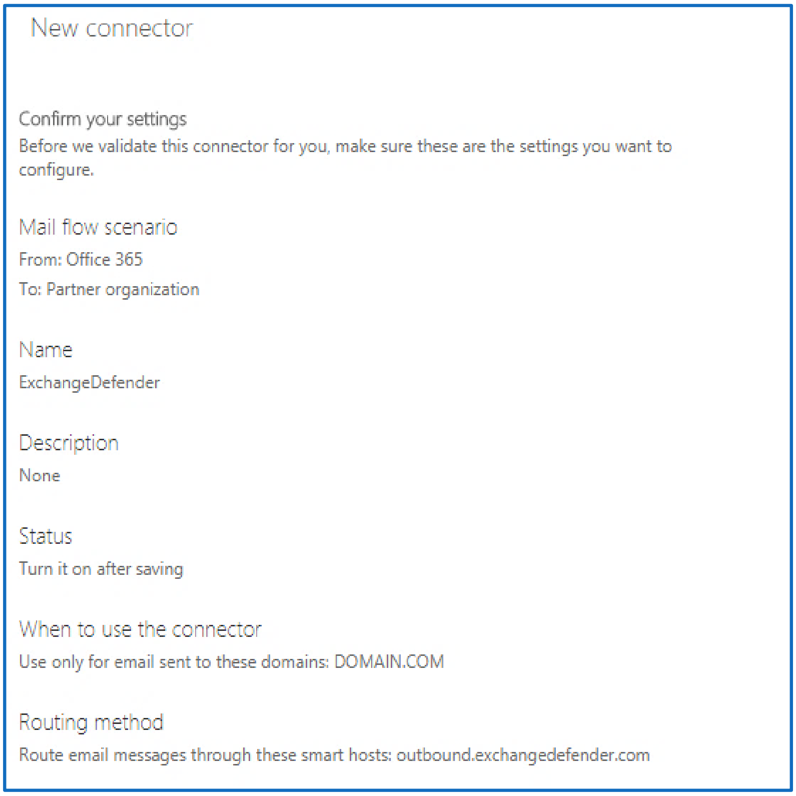
● Issued by a trusted certificate authority (CA)

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

Example: contoso.com or *.contoso.com

The issuing certificate authority (CA) is trusted by Microsoft. This option validates that the certificate is trusted.

Hit '**Next**' once the settings match what you see above. From here it'll ask you to **validate** your settings. You should see the following screen:



New connector

Confirm your settings
Before we validate this connector for you, make sure these are the settings you want to configure.

Mail flow scenario
From: Office 365
To: Partner organization

Name
ExchangeDefender

Description
None

Status
Turn it on after saving

When to use the connector
Use only for email sent to these domains: DOMAIN.COM

Routing method
Route email messages through these smart hosts: outbound.exchangedefender.com

Next, you'll be asked to validate that the connector works properly, so hit the '**+**' button to add a specific email to test it on.

Finally, once you've added the email hit '**Ok**' and on the next screen hit '**Validate**' and all should work as expected.

If anything goes wrong, recheck your settings and modify any mistakes in the settings and validate again.