

# A Basic User Guide:

# Office 365 Inbound and Outbound Configuration

## Table of Contents

<b>Overview.....</b>	<b>3</b>
Scope.....	3
Audience.....	3
Prerequisite.....	3
Assumptions.....	3
Additional Documents.....	3
<b>SMX Provisioning Process.....</b>	<b>4</b>
<i>Existing SMX customers migrating to Office 365.....</i>	<i>4</i>
<i>New SMX customers already using Office 365.....</i>	<i>4</i>
<b>Office 365 Inbound Email Configuration.....</b>	<b>5</b>
<i>Lock Down Port 25.....</i>	<i>5</i>
<i>Add Calendar Exceptions.....</i>	<i>8</i>
<i>Create Inbound Connector.....</i>	<i>10</i>
<i>Whitelist IP Addresses.....</i>	<i>13</i>
<b>Office 365 Outbound Email Configuration.....</b>	<b>14</b>
<i>Update SPF Record.....</i>	<i>14</i>
<i>Create Outbound Connector.....</i>	<i>15</i>

## Overview

This document will provide you with details on how to set up Office 365 inbound and outbound filtering with SMX products.

## Scope

This describes the process to set up SMX Email Security in combination with Microsoft Office 365 (Exchange Online). It covers the following cases:

1. Office 365 customer having their own email servers on premise;
2. Office 365 customer having some of their mailboxes hosted with Exchange Online, and some on their on-premise email servers;
3. All mailboxes hosted with Exchange Online.

## Audience

This document is designed for IT administrators who are setting up Office configuration with SMX. This can be used for new customers or for existing SMX customers.

## Prerequisite

Before proceeding with the steps below please ensure your account has been set up with SMX including inbound and outbound filtering. You will also need to have Shared Services added to your account if you wish to send emails out via SMX using Office 365.

## Assumptions

It is assumed that you have access to the Office 365 administration section so you can carry out the steps outlined below. It is also assumed that you have access to the SMX Portal to update the necessary SMX configuration.

## Additional Documents

Title	Summary
SMX Portal Administrator Guide	A detailed guide on how to administer the SMX portal.
SMX Inbound and Outbound Scrubbing Guide	Basic guide on how to use inbound and outbound filtering services.
SMX Security Plugins - Admin and User Guides	How to install the SMX plugin for spam submissions.

## SMX Provisioning Process

SMX can provision to existing customer who are migrating to Office 365 and to new customers already on Office 365. Before SMX can start the provisioning process in any of these customers, the customer has to set up and test the SMTP Relay (`yourcompany-com.mail.protection.outlook.com`) with Microsoft Office 365.

Once SMX has received the confirmation that this has been completed, SMX will initiate an SMTP connection with the customers' Mail Relay Host of "`yourcompany-com.mail.protection.outlook.com`".

If successful, SMX will then provision the customers' domain name(s) onto SMX's platform.

An email will be sent to the designated notification email address to confirm that the provisioning for the requested SMX service(s) has been completed.

The next step is to update the DNS MX records so all inbound email is relayed to SMX's servers. The MX records are:

10 mx1.nz.smxemail.com  
20 mx2.nz.smxemail.com

Please ensure there are no other MX records present.

After the DNS changes have been completed, SMX will immediately begin accepting email from the world, and deliver it to the defined Mail Relay Host that has been configured.

## Existing SMX customers migrating to Office 365

Once you have set up the mailboxes in your Office 365 configuration then please update the mail relay host in the portal to `yourcompany-com.mail.protection.outlook.com` and then carry on with steps below.

## New SMX customers already using Office 365

Please follow the steps below as outlined to ensure the successful set up of Office 365 with SMX.

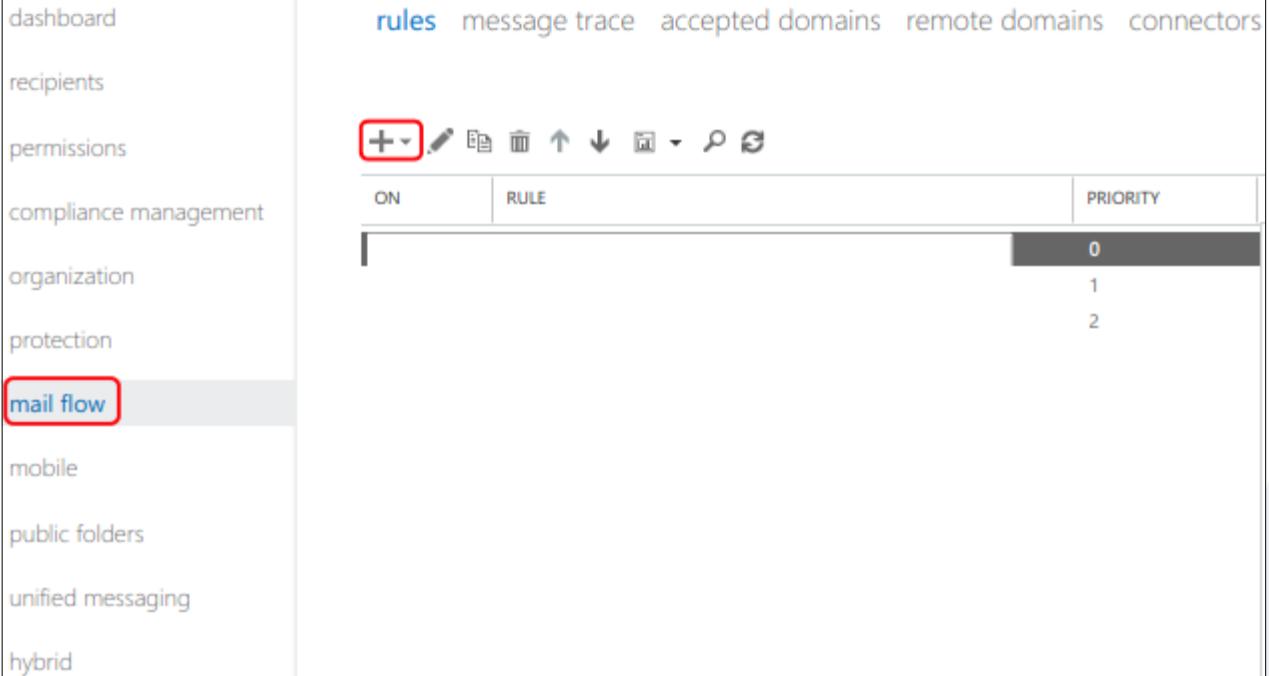
## Office 365 Inbound Email Configuration

### Lock Down Port 25

To ensure spammers cannot bypass SMX Filtering by sending spam directly to the customer's Office 365 mail server, SMX strongly recommends restricting inbound port 25 traffic except for the SMX IP ranges. Without this, the customer will not receive the full protection from SMX's service. This rule will help achieve this.

1. Go to Exchange Admin Center page (select **Admin | Exchange** from title bar).
2. Click **mail flow** from left navigation, select **rules**.
3. Click the **+** symbol

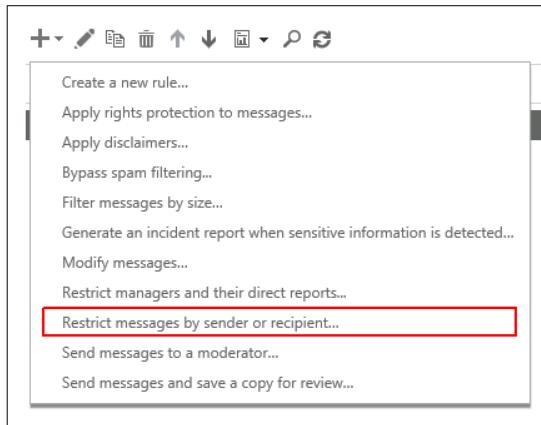
#### Exchange admin center



The screenshot shows the Exchange Admin Center interface. On the left, there is a navigation menu with links: dashboard, recipients, permissions, compliance management, organization, protection, **mail flow** (which is highlighted with a red box), mobile, public folders, unified messaging, and hybrid. On the right, there is a top navigation bar with links: rules, message trace, accepted domains, remote domains, and connectors. Below the top navigation is a toolbar with icons for creating, editing, deleting, and sorting rules. A table titled "rules" lists one rule with a priority of 0. The table has columns for ON, RULE, and PRIORITY.

ON	RULE	PRIORITY
ON		0
		1
		2

4. Select "**Restrict messages by sender or recipient...**" from pull-down menu.



5

v0.1

5. Name: "**Only accept inbound mail from SMX**"

6. Apply this rule if

- Choose **The sender is located**
- In the select sender location window, select **Outside the organization**
- Click OK

7. Do the following: **Delete the message without notifying anyone**

8. **Deselect** Audit this rule with severity level

9. Choose a mode for this rule: **Enforce** must be ticked

Name:  
Only accept inbound mail from SMX

\*Apply this rule if...  
The sender is located... Outside the organization

\*Do the following...  
Delete the message without notifying anyone

Properties of this rule:  
 Audit this rule with severity level:  
Not specified ▾

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

[More options...](#)

select sender location

Outside the organization

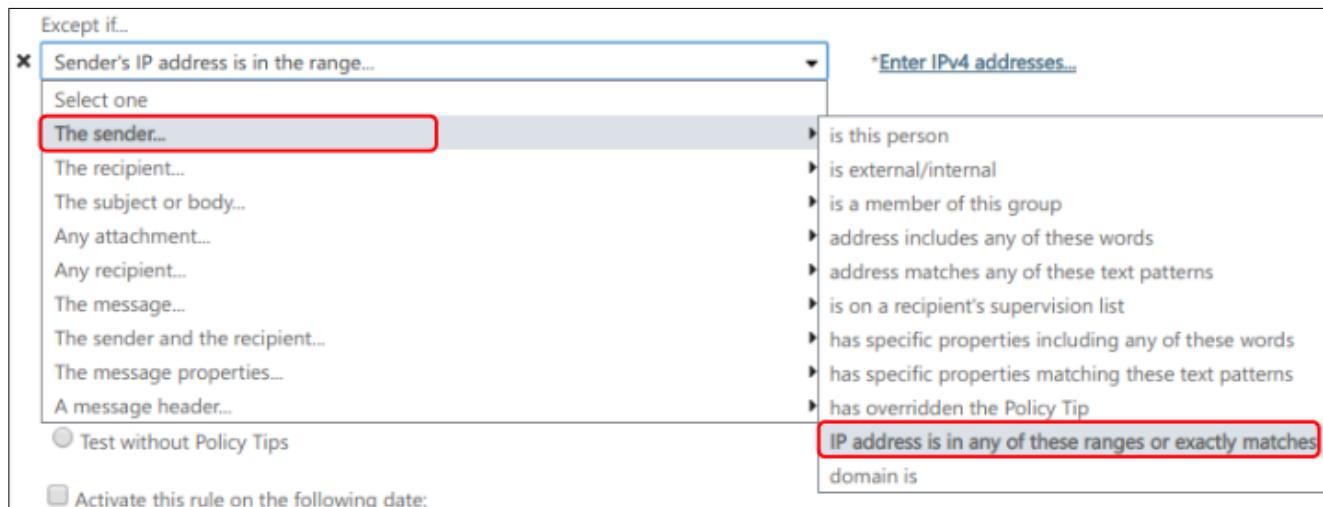
10. Click **More options** to show the rest of the window before proceeding to the next steps:

11. Under Except if, click add exception

Except if...

add exception

12. Select The sender... | IP address is in any of these ranges or exactly matches.



Except if...

Sender's IP address is in the range... \*Enter IPv4 addresses...

Select one

- The sender... The sender...
- The recipient...
- The subject or body...
- Any attachment...
- Any recipient...
- The message...
- The sender and the recipient...
- The message properties...
- A message header...

Test without Policy Tips

[Activate this rule on the following date:](#)

- ▶ is this person
- ▶ is external/internal
- ▶ is a member of this group
- ▶ address includes any of these words
- ▶ address matches any of these text patterns
- ▶ is on a recipient's supervision list
- ▶ has specific properties including any of these words
- ▶ has specific properties matching these text patterns
- ▶ has overridden the Policy Tip
- IP address is in any of these ranges or exactly matches IP address is in any of these ranges or exactly matches
- domain is

13. In the Specify IP address ranges window, enter the following IP Ranges:

113.197.64.0/24  
 113.197.65.0/24  
 113.197.66.0/24  
 113.197.67.0/24  
 203.84.134.0/24  
 203.84.135.0/24

14. Click the add icon for each range

15. Click OK, then Save.

The window should look like the screenshot on the next page:

Except if...

Sender's IP address is in the range... [Enter IPv4 addresses...](#)

Properties of this rule:

Audit this rule with severity level:  
Not specified

Choose a mode for this rule:

Enforce  
 Test with Policy Tips  
 Test without Policy Tips

Activate this rule on the following date:  
Thu 17/01/2019 3:00 PM

Deactivate this rule on the following date:  
Thu 17/01/2019 3:00 PM

Stop processing more rules  
 Defer the message if rule processing doesn't complete

Match sender address in message:  
Header

Comments:

Save Cancel

specify IP address ranges

+

113.197.67.0/24  
113.197.66.0/24  
113.197.65.0/24  
113.197.64.0/24  
203.84.135.0/24  
203.84.134.0/24

OK Cancel

## Add Calendar Exceptions

To ensure calendar invites are not rejected it is a good idea to also add an exception to the rule. To do this please follow these steps:

1. Click on add exception

Except if...

Sender's IP address is in the range... ▼

- ['113.197.67.0/24' or](#)
- ['113.197.66.0/24' or](#)
- ['113.197.65.0/24' or](#)
- ['113.197.64.0/24' or](#)
- ['203.84.135.0/24' or](#)
- ['203.84.134.0/24'](#)

**add exception**

2. Choose "**The message properties**" and "**include the message type**"

or

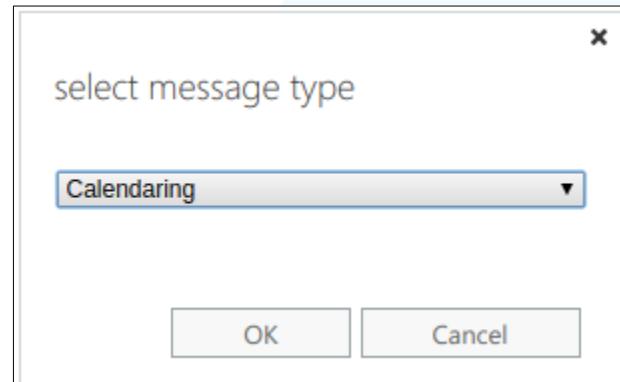
The message type is... \*Select one...

Select one

The sender...  
The recipient...  
The subject or body...  
Any attachment...  
Any recipient...  
The message...  
The sender and the recipient...  
**The message properties...** ► include the message type  
A message header...  
 Test without Policy Tips  
 Activate this rule on the following date:

► include this classification  
don't include any classification  
include an SCL greater than or equal to  
include the importance level

3. Select **Calendaring** and click on OK



4. Then the exception will be completed

Except if...

Sender's IP address is in the range... ▼

['113.197.67.0/24' or](#)  
['113.197.66.0/24' or](#)  
['113.197.65.0/24' or](#)  
['113.197.64.0/24' or](#)  
['203.84.135.0/24' or](#)  
['203.84.134.0/24'](#)

or

The message type is... ▼

[Calendaring](#)

[add exception](#)

## Create Inbound Connector

To create a connector in Office 365

1. Still from **mail flow**, click **connectors**.

If any connectors already exist for your organisation, you can see them listed here.

[Exchange admin center](#)

dashboard    recipients    permissions    compliance management    organization    protection    **mail flow**    mobile    public folders    unified messaging    hybrid

rules    message trace    accepted domains    remote domains    **connectors**

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first [check to see if you should create a connector](#).

Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

STATUS	NAME	FROM	TO
Off	Inbound email from SMX	Partner organization	Office 365
On	SMX	Office 365	Partner organization

**+  **

**Inbound email from SMX**

Mail flow scenario  
From: Partner organization  
To: Office 365

Description  
Inbound email from SMX

2. To start the wizard, click the plus (+) symbol.

3. Click **Next**, and follow the instructions in the wizard.

- a) From: **Partner organization**
- b) To: **Office 365**

## 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.

Next

Cancel

4. Give the connector a name e.g. SMX

## New connector

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

\*Name:

**SMX**

Description:

(Empty text area)

What do you want to do after connector is saved?

Turn it on

Next

Cancel

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

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.

[Back](#) [Next](#) [Cancel](#)

6. Add the following IP address ranges:

Specify the sender IP address range.

+  -

- 203.84.134.0/24
- 203.84.135.0/24
- 113.197.64.0/24
- 113.197.65.0/24
- 113.197.66.0/24
- 113.197.67.0/24

Specify IP address ranges that this connector applies to.

[Back](#) [Next](#) [Cancel](#)

7. Then go to the next screen, ensure **Reject email messages if they aren't sent over TLS** is **ticked**, then click **Next**

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 ...

[Back](#) [Next](#) [Cancel](#)

8. Confirm everything is correct before clicking **Save**.

Confirm your settings  
Before saving, make sure these are the settings you want to configure.

Mail flow scenario  
From: Partner organization  
To: Office 365

Name  
SMX

Description  
None

Status  
Turn it on after saving

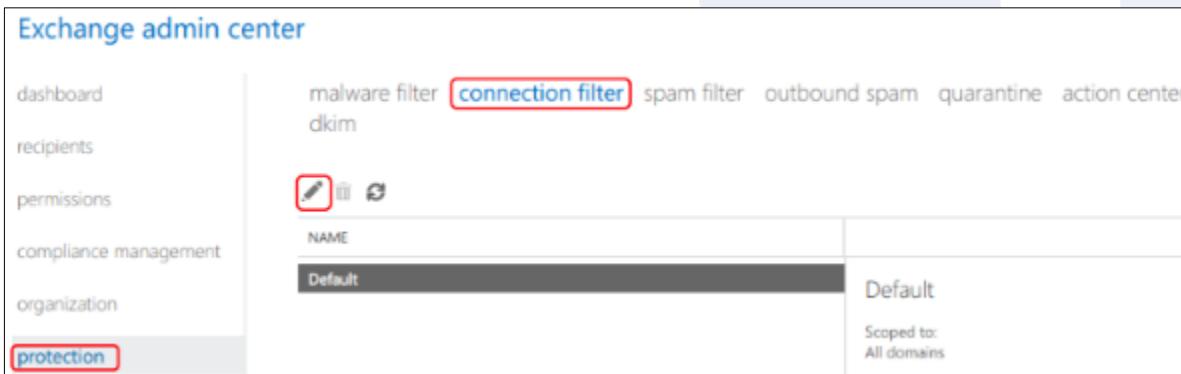
How to identify your partner organization  
Identify the partner organization by verifying that messages are coming from these IP address ranges:  
203.84.134.0/24,203.84.135.0/24,113.197.64.0/24,113.197.65.0/24,113.197.66.0/24,113.197.67.0/24

Security restrictions  
Reject messages if they aren't encrypted using Transport Layer Security (TLS).

## Whitelist IP Addresses

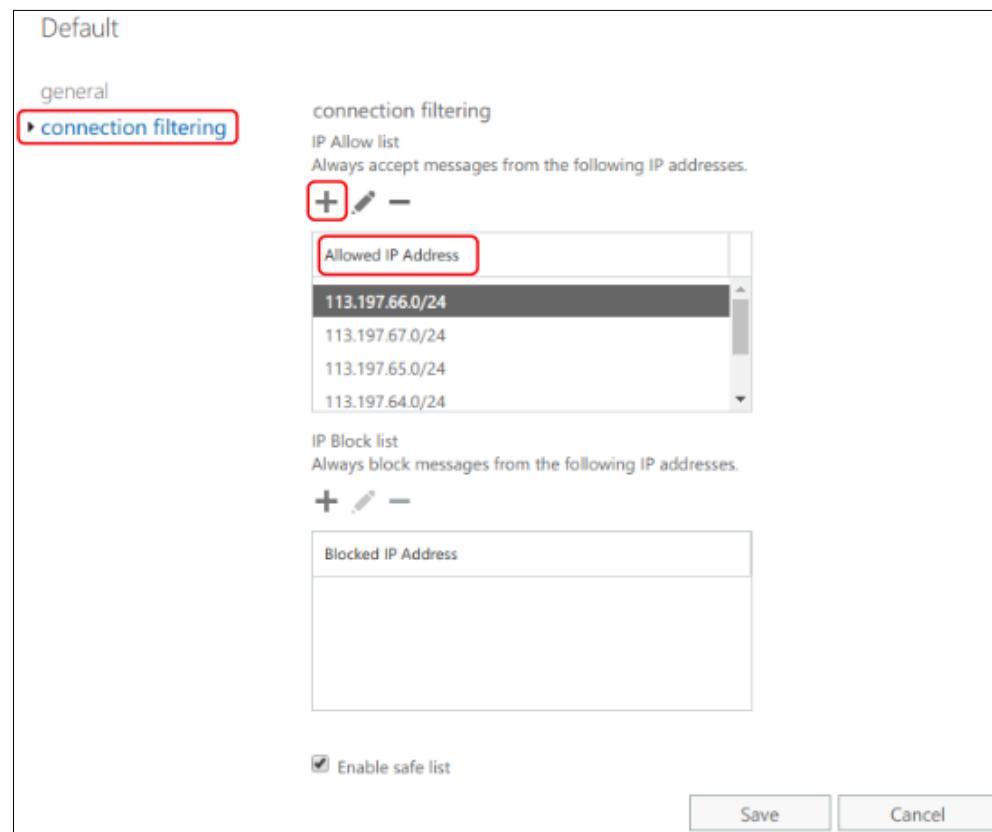
To avoid emails that pass through SMX from being rate limited, follow these steps:

1. Click on **Protection** from the left-hand panel



The screenshot shows the Exchange admin center interface. On the left, there's a sidebar with links: dashboard, recipients, permissions, compliance management, organization, and protection. The 'protection' link is highlighted with a red box. At the top, there's a navigation bar with links: malware filter, connection filter (highlighted with a red box), spam filter, outbound spam, quarantine, action center, and dkim. Below the navigation bar, there's a table with columns for NAME, Action, and Scoped to. The first row shows 'Default' in the NAME column, 'Default' in the Action column, and 'All domains' in the Scoped to column.

2. Click on **Connection Filter**, then click the **Edit** icon
3. Click **Connection Filtering** then click the **Add** icon within the IP Allow list section and add the following IP ranges, then save



## Office 365 Outbound Email Configuration

**Important:** SMX Shared Services should be added under your SMX customer account before the steps below are completed.

### Update SPF Record

If your organisation has an SPF record, the DNS TXT record must be updated to include the following:

include:spf.nz.smxemail.com

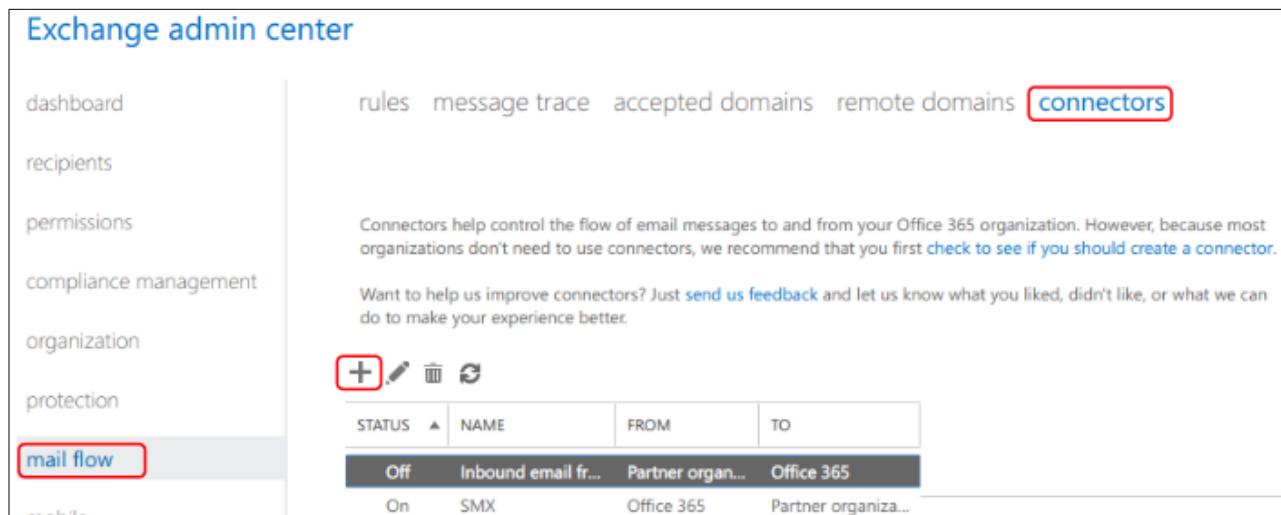
An example of the new SPF record is below:

- **Before:** v=spf1 include:spf.protection.outlook.com -all
- **After:** v=spf1 include:spf.protection.outlook.com include:spf.nz.smxemail.com -all

## Create Outbound Connector

To configure Microsoft Office 365 / Exchange Online to route outbound email via SMX Email Security:

1. From the **mail flow** on the left panel, select **connectors** (all existing connectors will then be displayed). Click on the plus icon (+) to add a new connector



**Exchange admin center**

rules message trace accepted domains remote domains **connectors**

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first [check to see if you should create a connector](#).

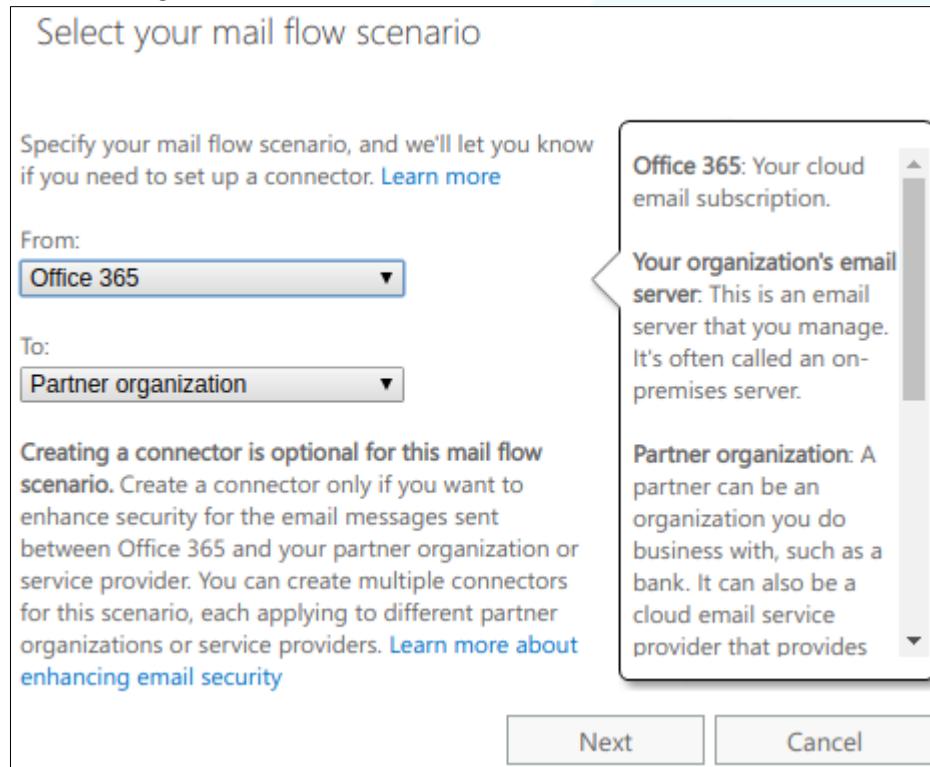
Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

STATUS	NAME	FROM	TO
Off	Inbound email fr...	Partner organ...	Office 365
On	SMX	Office 365	Partner organiza...

2. Under Select your mail flow scenario, select the following then click the Next button

**From:** Office 365

**To:** Partner organization



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

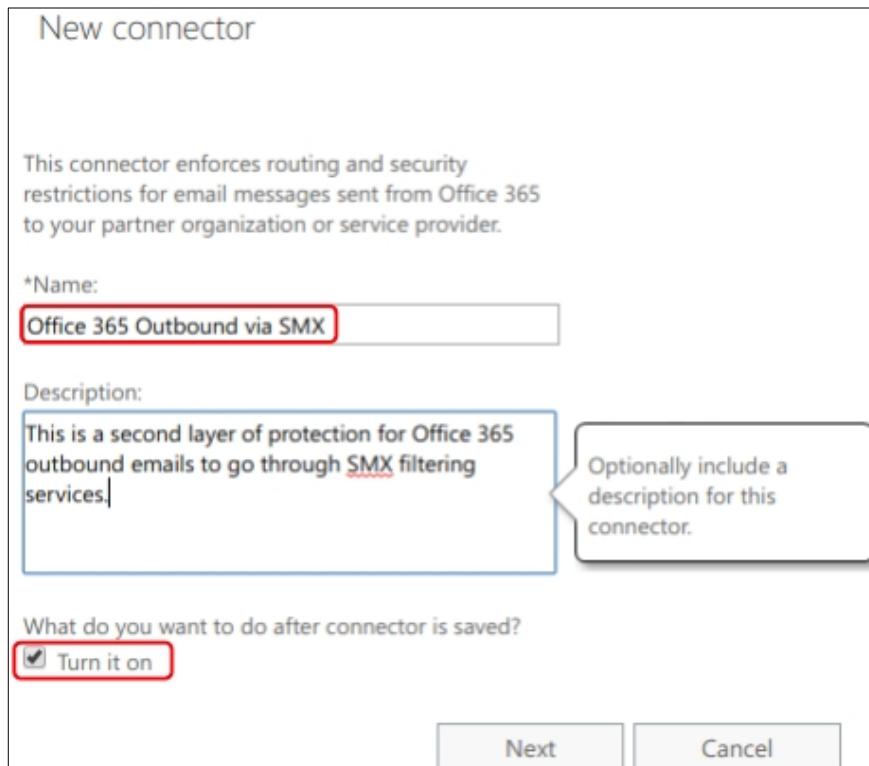
Next Cancel

3. Complete the New Connector - New Connector dialog as follows:

**Name:** Type preferred connector name i.e. Office 365 Outbound via SMX

Description: Optional

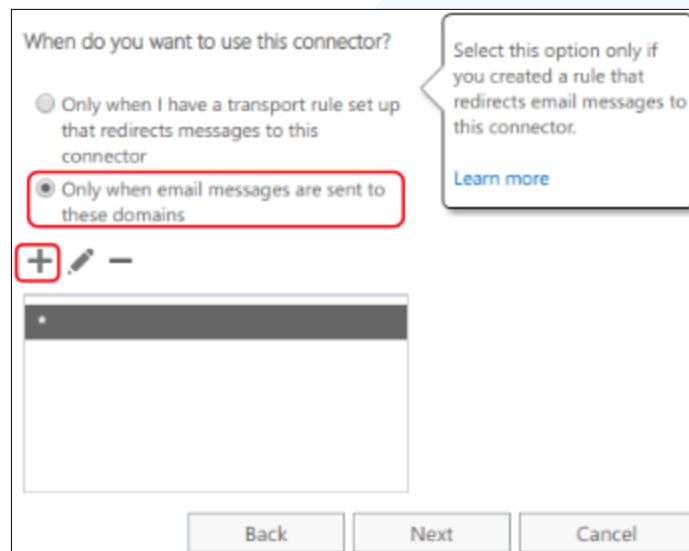
**Tick** "What do you want to do after connector is saved?"



Next

Cancel

4. Choose **Only when email messages are sent to these domains** option, and then click the (+) plus symbol
5. Enter a value of **\* (asterisk)** to route all outbound emails through SMX. Click the **OK** button, then the **Next** button

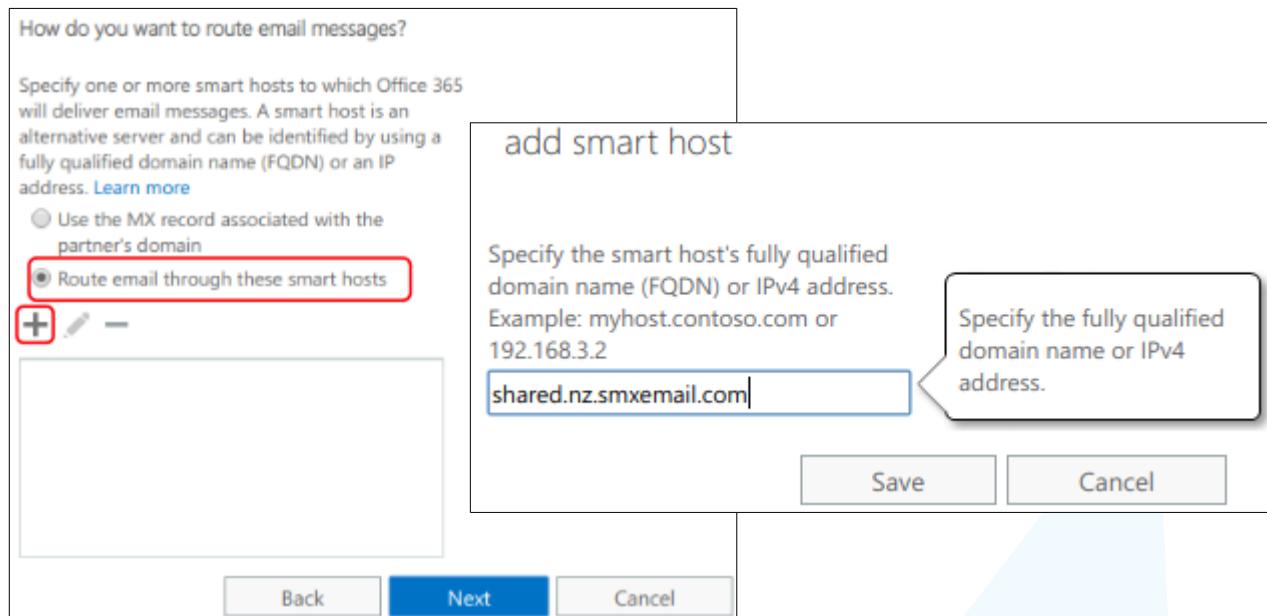


Back

Next

Cancel

6. Select **Route email through these smart hosts**, and then click on the (+) plus symbol



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

**+** **-**

shared.nz.smxemail.com

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

Save Cancel

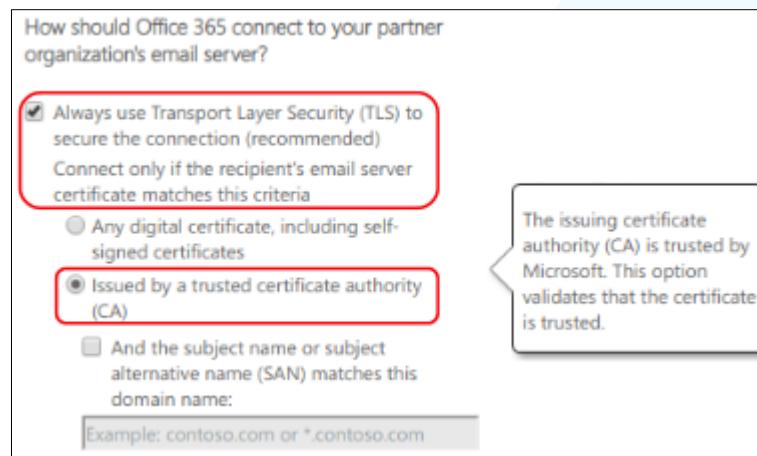
Back Next Cancel

7. Type in **shared.nz.smxemail.com**, Click **Save**, and then click **Next**

8. Select the following options then click the **Next** button to verify your settings:

- Always use Transport Layer Security (TLS) to Secure the Connection (recommended)
- Issued by a trusted certificate authority (CA)

9. Add an email address of a recipient from a domain external to your organisation then click the **Validate** button 19. Once Office 365 has successfully validated your settings, click the **Save** button.



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.

## Contact SMX

SMX values your feedback. If you have comments about this guide, please send an email message to [emailsupport@smxemail.com](mailto:emailsupport@smxemail.com). In your email message, please specify the document name and the section to which your comment applies. If you want to receive a response to your comments, ensure that you include your name and contact information.