Office 365 Inbound and Outbound SMX configuration

4th January 2018

Legal Notice

The contents of this document constitute valuable proprietary and confidential property of SMX Limited and are provided subject to specific obligations of confidentiality set forth in one or more binding legal agreements. Any use of this material is limited strictly to the uses specifically authorised in the agreement(s) pursuant to which such material has been furnished. Any use or disclosure of all or any part of this material not specifically authorised in writing by SMX Limited is strictly prohibited.

Re-Distribution Prohibited

This document may not be re-distributed without the prior written consent of SMX Limited.

SMX and the SMX logo are registered trademarks and/or trademarks of SMX Limited in various jurisdictions. All other trademarks are the properties of their respective owners.

For further information see: www.smxemail.com

Inbound configuration

This describes the process to set up SMX Cloud Email Security in combination with 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.

SMX Provisioning Process

Before SMX can start the provisioning process, the customer has to set up and test the SMTP Relay (yourcompany-com.mail.protection.outlook.com) with 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 the 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 completed, SMX will immediately begin accepting email from the world, and deliver it to the defined Mail Relay Host that has been configured.

Office 365 Setup Guide

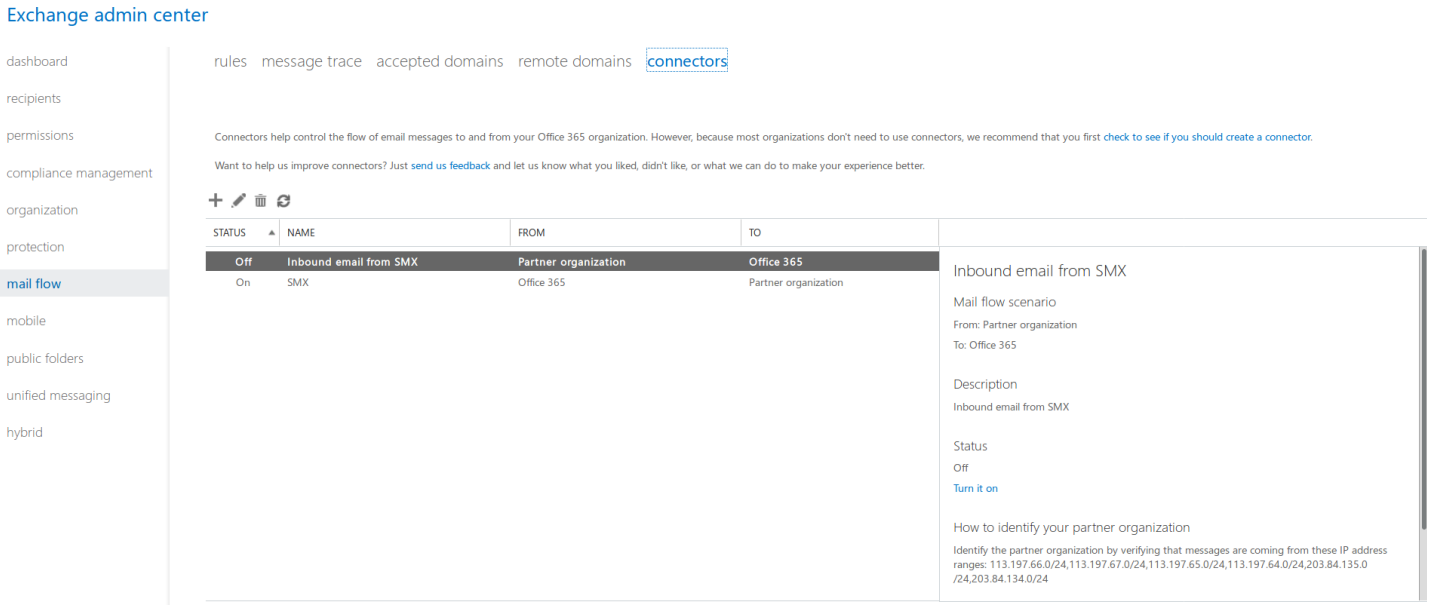
To ensure spammers cannot bypass SMX Filtering by sending spam directly to the customer's Office635 mail server, SMX strongly recommends restricting inbound port 25 traffic for all except these IP address ranges:

203.84.134.0/23 (203.84.134.0 to 203.84.135.255)
113.197.64.0/22 (113.197.64.0 to 113.197.67.255)

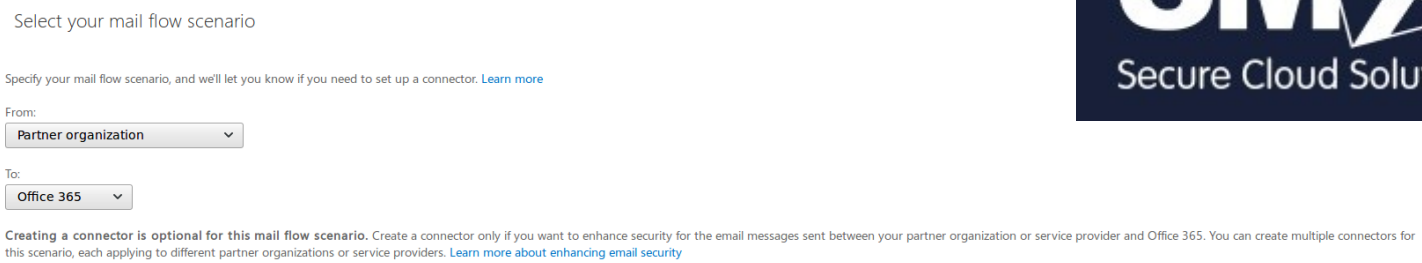
Without this, the customer will not receive the full protection from SMX's service. These are the steps to configure Office 365 for SMX Cloud Email Security:

Step 1 Creating a connector for Office 365

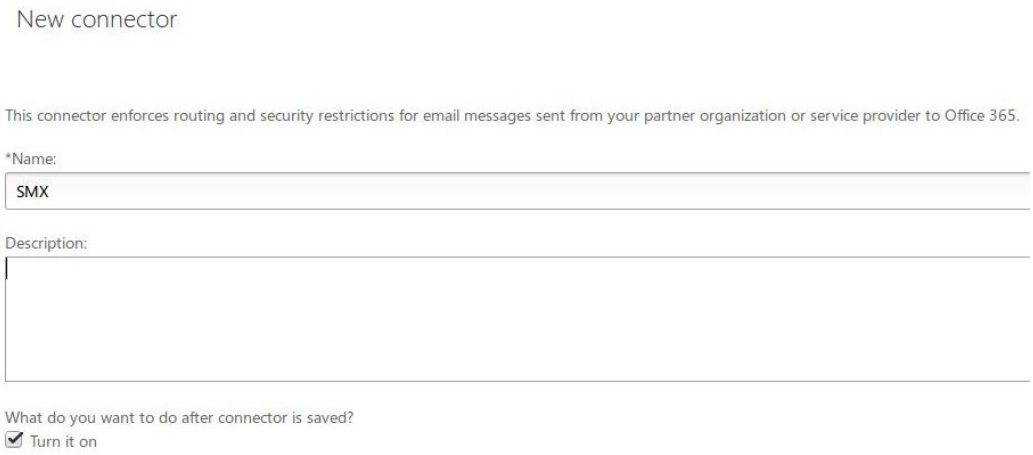
To create a connector in Office 365, click **Admin**, and then click **Exchange** to go to the **Exchange Admin Center**. Next, click **mail flow,** and click connectors. If any connectors already exist for your organisation, you can see them listed here.



To start the wizard, click the plus (+)symbol. Click **Next**, and follow the instructions in the wizard.



Give the connector a name e.g. SMX

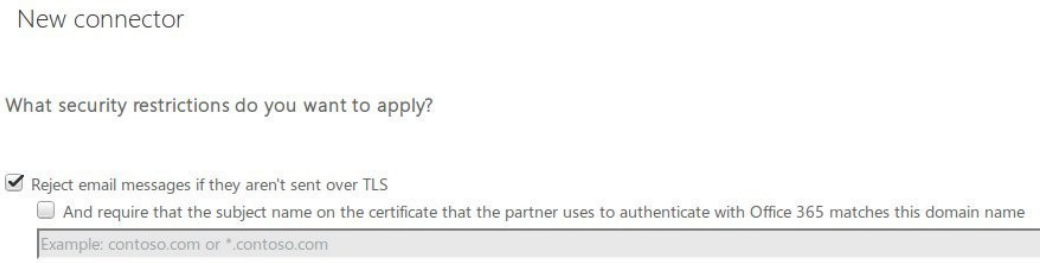


Choose **Use the sender's IP address**

Add the following IP 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

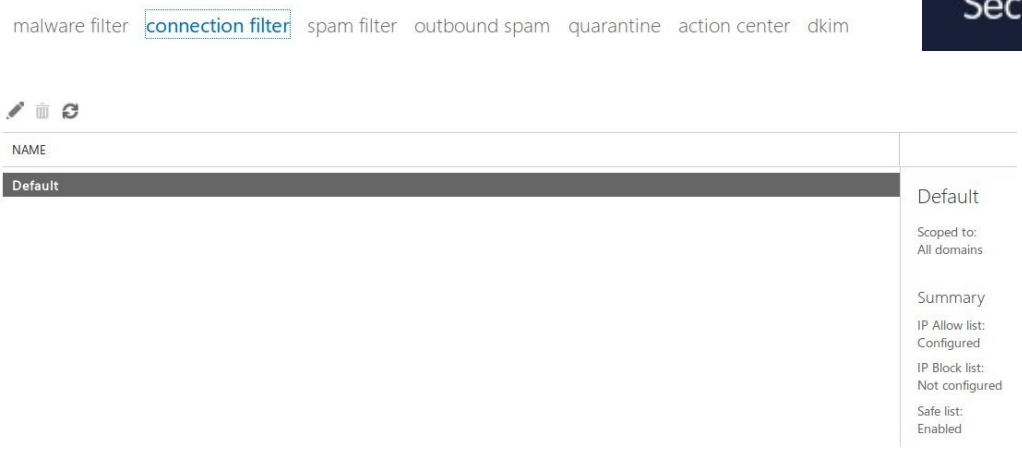
Then go to the next screen



The settings can then be saved.

Step 2 Whitelisting with Office 365

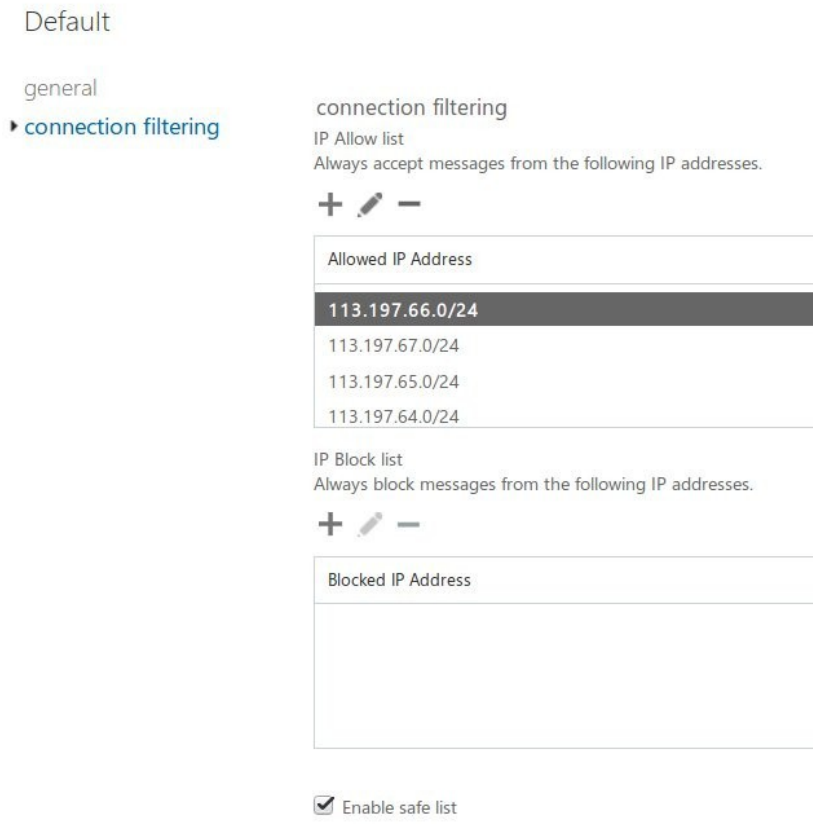
- Login to the Office 365 Exchange Admin Center (EAC)
- Click on **Protection**
- Click on **Connection Filter**, then click the **Edit** icon



Click **Connection Filtering** then click the **Add** icon within the IP Allow list section and add the following IP 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

Then click on save.



Outbound Configuration

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

Microsoft Office 365 Outbound Email Configuration

Prerequisite:

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:

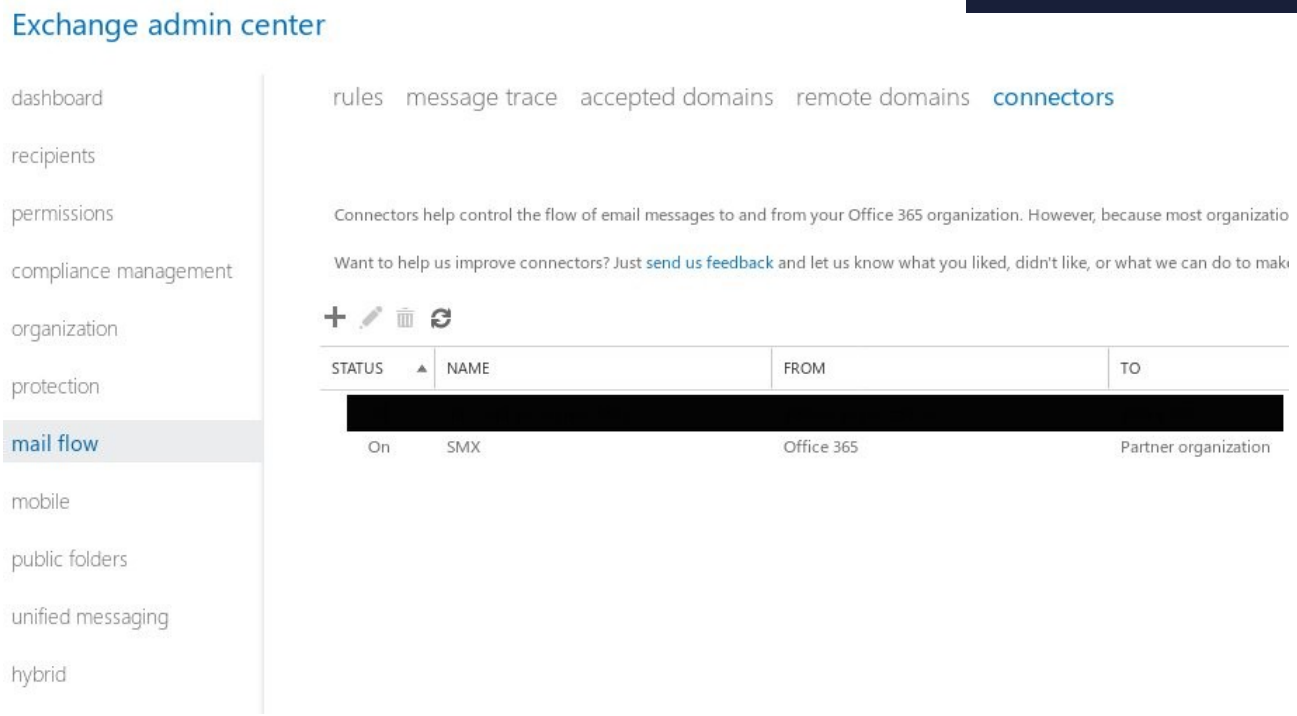
- **Before:** v=spf1 include:spf.protection.outlook.com -all
- **After:** v=spf1 include:spf.protection.outlook.com include:spf.nz.smxemail.com -all

Configuration Steps:

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

1. Log in to the Microsoft Office 365 portal
2. Go to **Admin** → **Admin centers** on the left pane → **Exchange**
3. Select **mail flow** on the left pane → **connectors**

   All existing connectors will then be displayed



- Click on the plus icon (**+**) to add a new connector

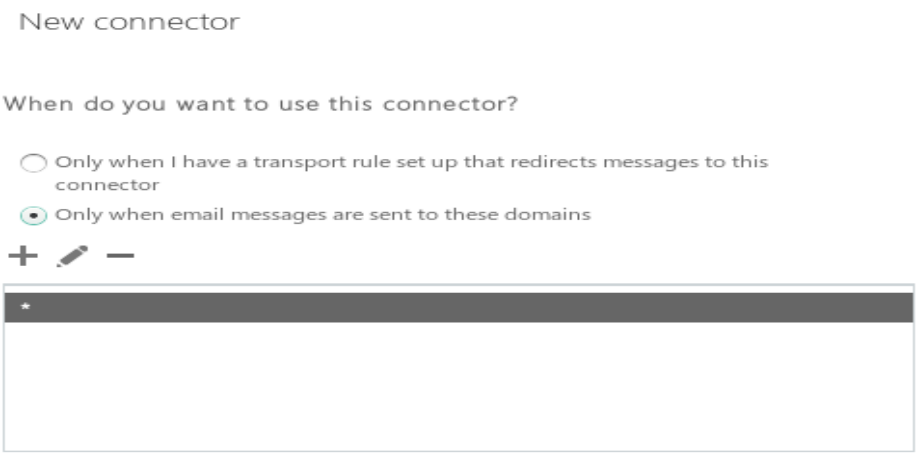
5. Under Select your mail flow scenario, select the following:

   From: Office 365
   To: Partner organization

6. Click the **Next** button
7. Complete the New Connector - New Connector dialog as follows:

Field	**Description**
Name	Enter a name for the Connector.
Description	Optionally, give an informative description for the Connector.
Turn it On	Select this option to enable the Connector.

8. Choose **Only when email messages are sent to these domains** option, and then click the plus icon (**+**)
9. Enter a value of * **(asterisk)** to route all outbound emails through SMX



10. Click the **OK** button

11.Click the **Next** button

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

13. Type in ***shared.nz.smxemail.com***

14. Click **Save**, and then click **Next**

15**.** Select the following options:

Always use Transport Layer Security (TLS) to Secure the Connection (recommended)

Issued by a trusted certificate authority (CA)

16. Click the **Next** button to verify your settings

17. Add an email address of a recipient from a domain external to your organisation

18. Click the **Validate** button

19. Once Office 365 has successfully validated your settings, click the **Save** button.