

Office 365 Inbound and Outbound SMX configuration

4th January 2018

Legal Notice

Copyright © 2005-2018 SMX Limited. All rights reserved.

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 Office365 mail server, SMX strongly recommends restricting inbound port 25 traffic for all except these IP address ranges:

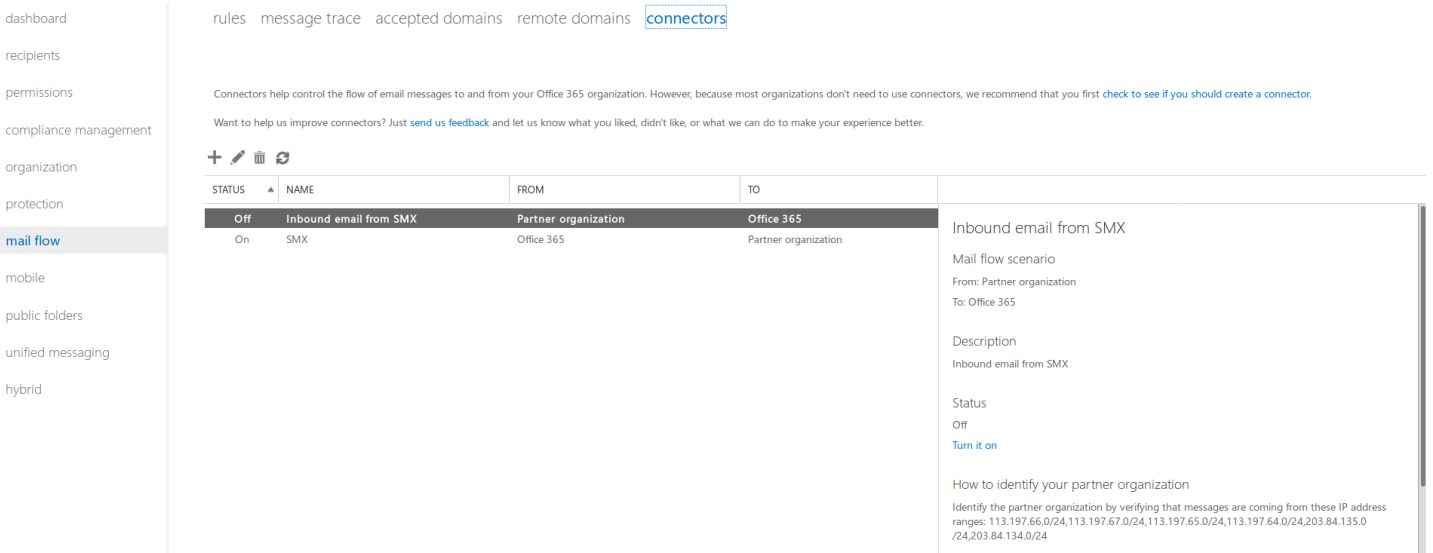
- 203.84.134.0/23 (203.84.134.0 to 203.84.135.255)
- 113.197.64.0/22 (113.197.64.0 to 113.197.67.255)

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.

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 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

Status
Off
[Turn it on](#)

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

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

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](#)

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:

What do you want to do after connector is saved?

Turn it on

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

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

New connector

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

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

Then go to the next screen

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

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



NAME	
Default	<p>Default</p> <p>Scoped to: All domains</p> <p>Summary</p> <p>IP Allow list: Configured</p> <p>IP Block list: Not configured</p> <p>Safe list: Enabled</p>

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.

Default

general

▶ **connection filtering**

connection filtering

IP Allow list

Always accept messages from the following IP addresses.



Allowed IP Address
113.197.66.0/24
113.197.67.0/24
113.197.65.0/24
113.197.64.0/24

IP Block list

Always block messages from the following IP addresses.



Blocked IP Address

Enable safe list

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

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 have a large number of external domains, it's difficult to manage them all. 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 it better.



STATUS	NAME	FROM	TO
On	SMX	Office 365	Partner organization

- 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

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

+ ✎ -

A screenshot of a text input field in a software interface. The field is empty and has a thin border. Above the field, there are three small icons: a plus sign, a pencil, and a minus sign.

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.