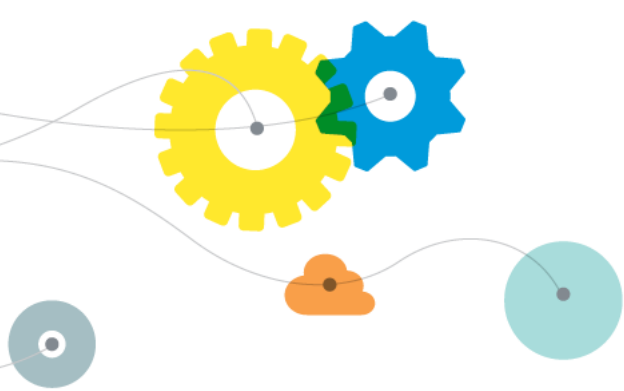# iMail Outbound Connector for Office365 Setup Guide for Securemail Premium –ver 1.1

1. Purpose

The purpose of this document is to detail how to set-up SYNAQ Securemail Premium on Office 365.

2. iMailSecuremail Premium – O365 Set-up

## 2.1. Step 1 – DNS Changes

Before iMail Securemail Premium can be set-up within O365, an addition to your existing SPF record already in place for O365, needs to be added.

- Add the following entry to your SPF record:
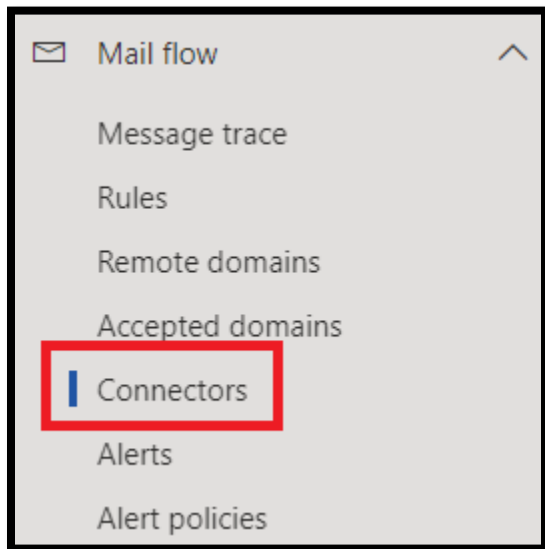
"v=spf1 include:_spf-securemail.synaq.com -all"

2.2. Step 2 – Configuring the Securemail Premium Connector

- Login to your O365 portal and click on drop down "*Admin Center*" on the left-hand side of your screen
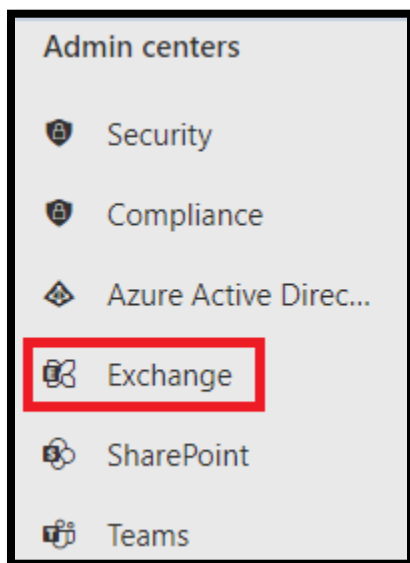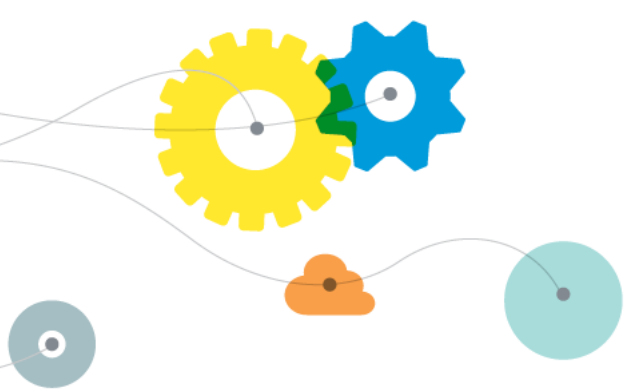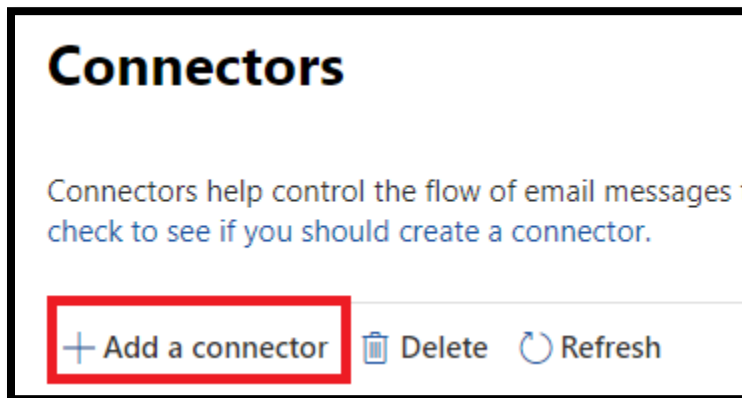
- Click on the the "Mail Flow" drop down from your menu and click on *"Connectors"*

- Click on "*+Add a connector*" sign to create new connector.

- A window will pop up to specify the mail flow scenario

- Select – From: "Office365" and To: "Partner Organization"

New connector

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

Connection from

◉ Office 365

○ Your organization's email server

○ Partner organization

Connection to

○ Your organization's email server

◉ Partner organization

- Click "Next".

- A new window will pop up requesting you to name the connector (we recommend using "imail Securemail Premium" for correct reference in future).

Connector name

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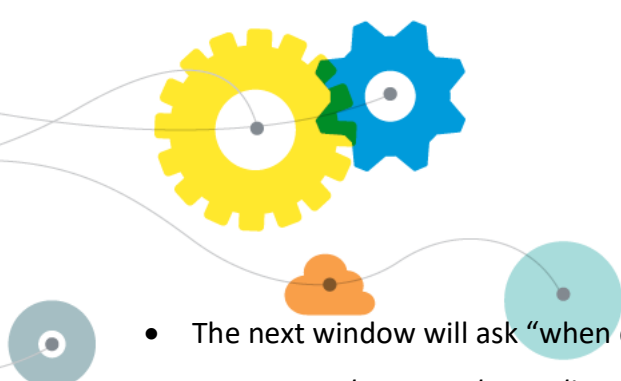
Name *

> SYNAQ Securemail Premium

Description

What do you want to do after connector is saved?

☑ Turn it on

- Select "*Next*".

- The next window will ask "when do you want to use the connector?" Select *"Only when I have a transport rule set up that redirects messages to this connector"* option.

Use of connector

Specify when 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

- Click "*Next*".
- Select the *"Route email through these smart hosts"* option and input iMail. smart host

  smtp-securemail.synaq.com

Routing

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.

- ◯ Use the MX record associated with the partner's domain
- ⦿ Route email through these smart hosts

  | smtp-securemail.synaq.com | + |

- Click on the blue plus button to confirm the use of the iMail Smart Host

Routing

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.

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

● Route email through these smart hosts

Example: myhost.contoso.com or 192.168.3.2   **+**

smtp-securemail.synaq.com

- Click "Next".

- The next screen will ask, "How should Office 365 connect to your partner organization's email server?" Select the "Always use Transport Layer Security (TLS) to secure the connection (recommended)" option.
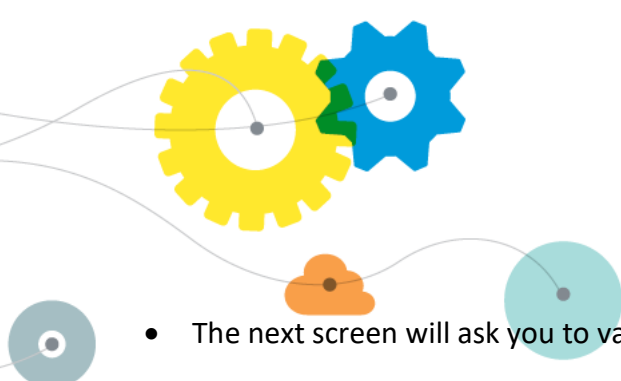
Security restrictions
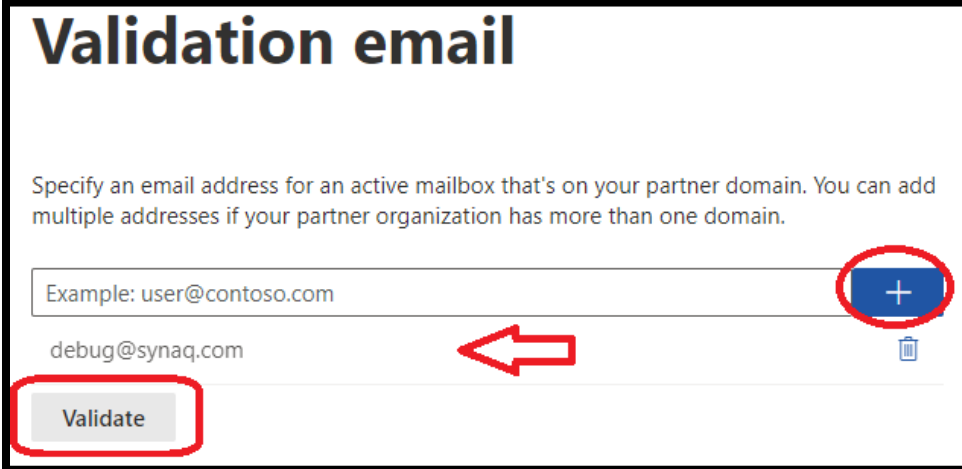
How should Office 365 connect to your partner organization's email server?

☑ 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

- Click "*Next*"

- The next screen will ask you to validate the connector.

- Input an external mail address, example: debug@synaq.com and click on the blue plus button to add that email for validation usage.

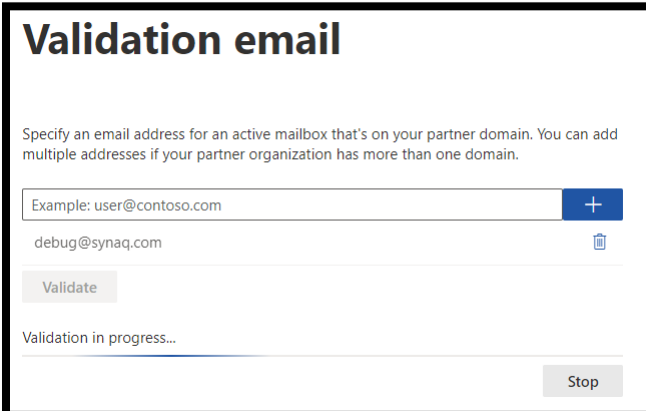- Click on *"Validate"* to verify the Connector settings.

- Validation in progress is what you will see next

- Please note: even though the validation will fail, this is not a concern and does not cause any issues. Click on *Next* to continue
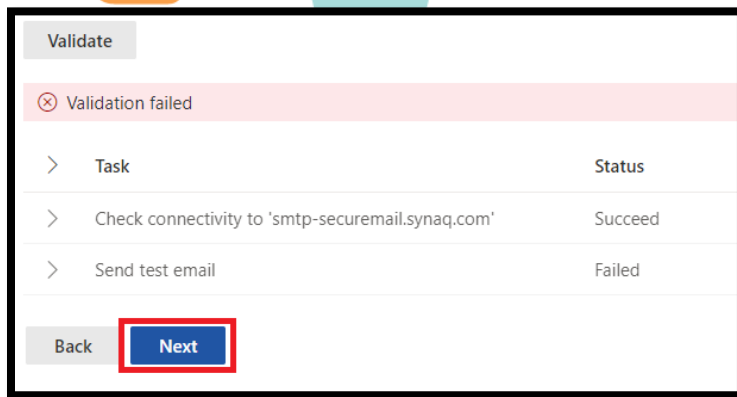
- Since it failed validation, you will be prompted to confirm that "*Do you really want to go without successful validation?*" Please click on *YES* to accept and proceed.
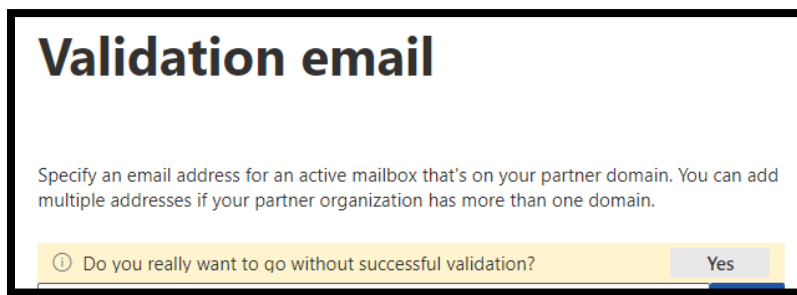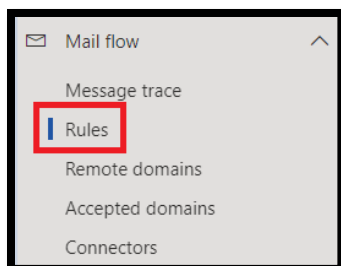

- Finally click on "*Create Connector*" which will now be used for the next section.

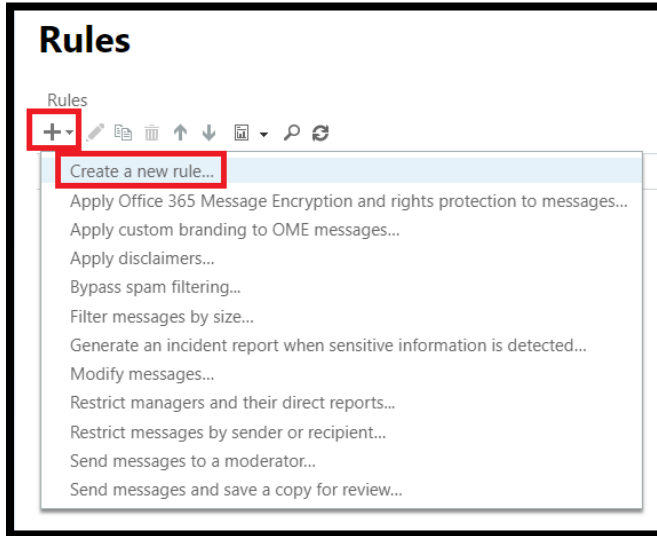## 2.3.   Step 3 – Creating Securemail Premium Transport Rule

In order to make use of the Send Connector we just created in point 2.2. Transport layer rules will need to be put in place to re-direct the mail correctly to the Send Connector.
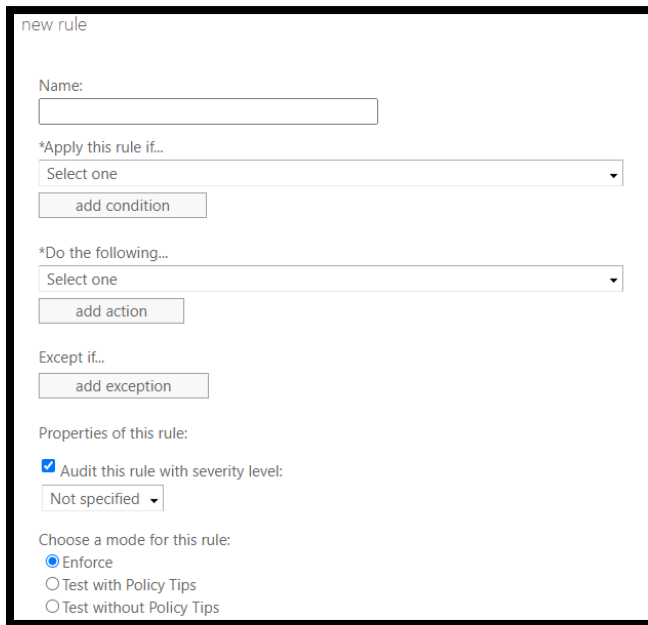
- Select "*Rules*" from the drop-down menu "*Mail Flow*"

- Select the "**+**" sign and choose the "create new rule" option.

- A "new rule" window will pop up. Click on **"more options"** at the bottom of the window (if you do not click on this, you will not be presented with all of the relevant options to configure the rule).

- Input/select the following information:

- Name: Input "iMail Securemail Premium Rules"

- Apply this rule if: Select "The sender" and "domain is"
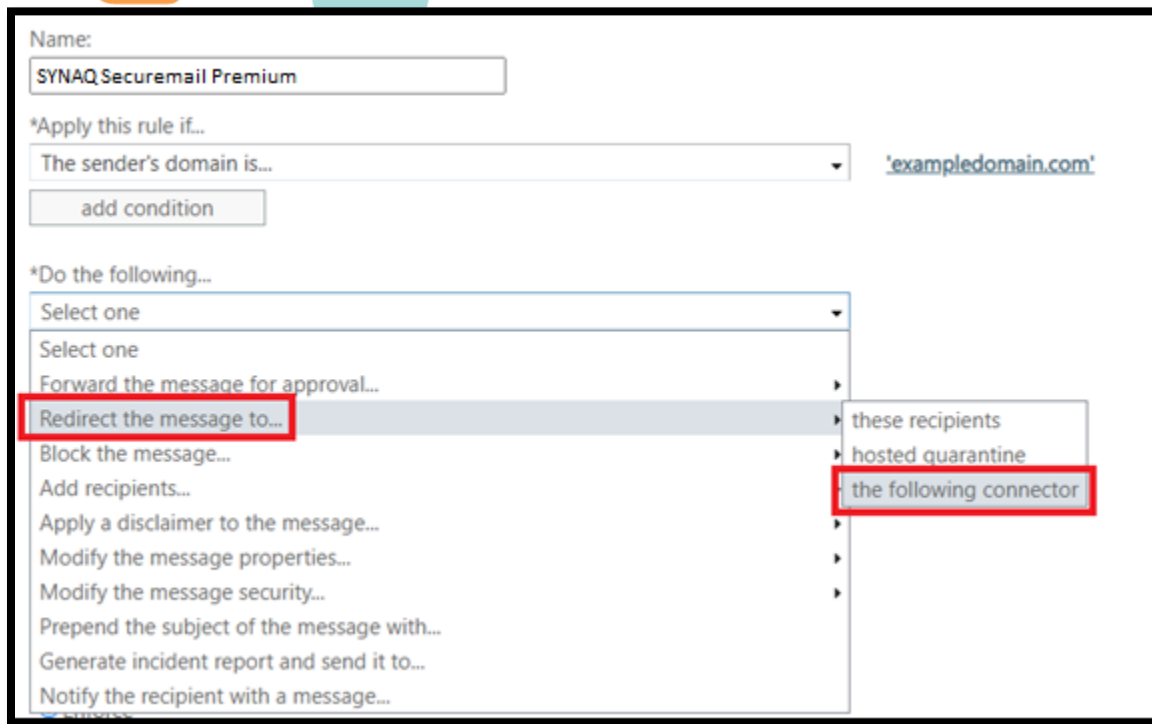

- This will prompt a new window requesting you to "specify domain".

- Input your own company domain, that require the mail to be routed to the Send Connector
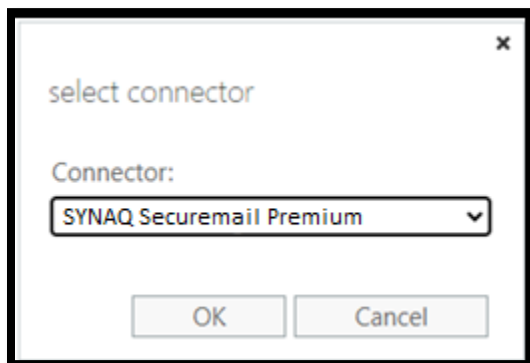
- Click the "+" sign and then click "ok".

- Under the "Do the following" option, select "redirect the messages to" and select "the following connector".
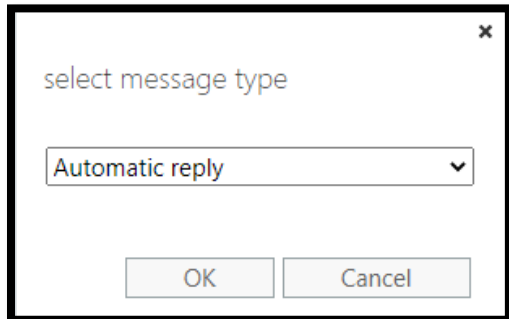
- Click on the "Select One" option on the right and select the "iMail Securemail Premium" Connector.

- We will need to add a few "*Exceptions*" to bypass certain replies from being sent through the Connector

- Click "*Add Exception*" and choose options "*The Message Properties*" -> "*Include the Message Type*"
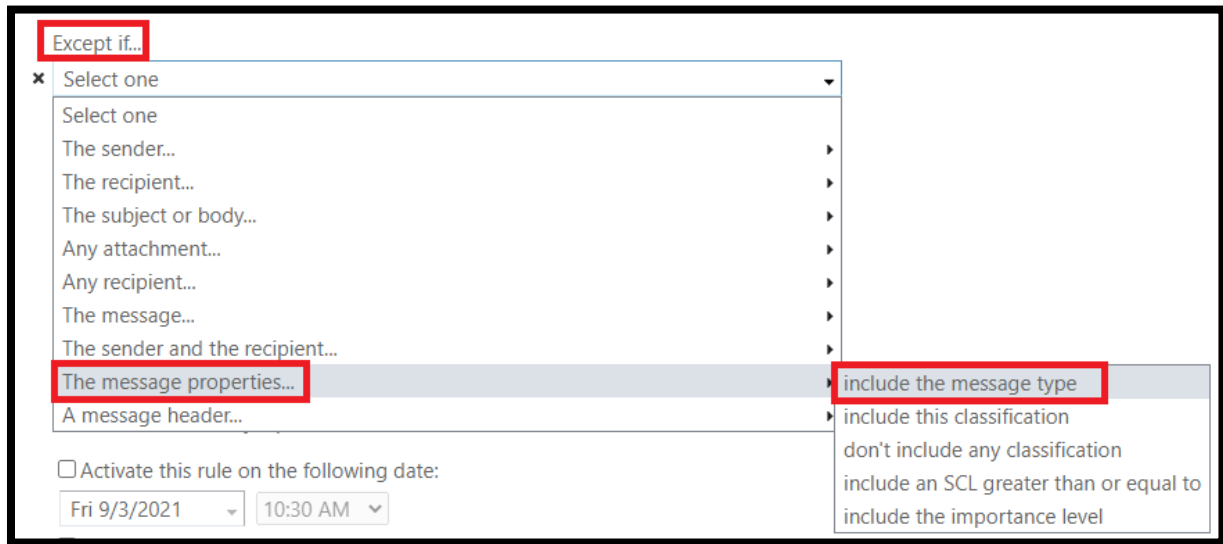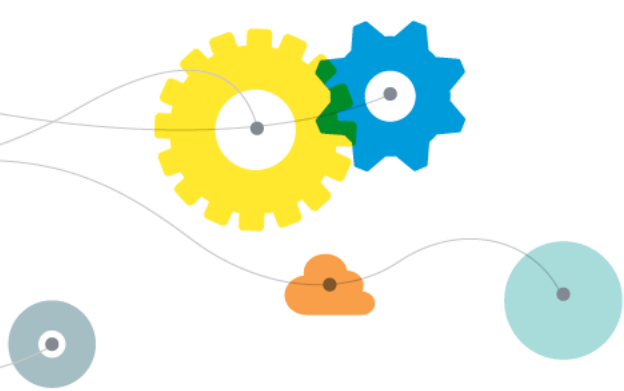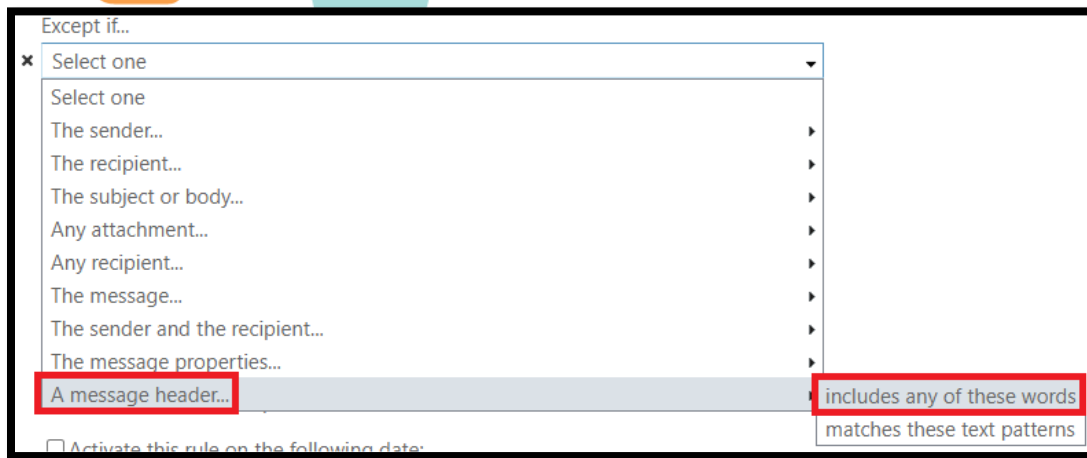
- Choose from the list *"Automatic Reply"* and click on OK

- Next, we will need to add extra Exception rules to make sure mails are Branded.

- Select in additional exception *"A Message Header"* -> *"includes any of these words"*
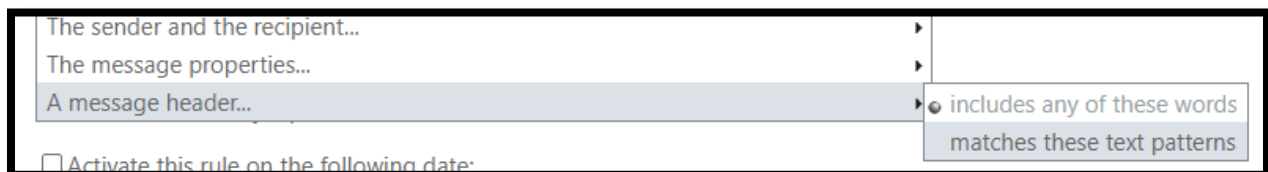
- You will now be required to specify the words by clicking on the "Enter text" and "Enter words" options on the right.

- Under the "Enter text" option, input:

- "X-SYNAQ-Pinpoint-Branding"

- Under the "Enter words" option, input:

- "Branded".

- Once saved, your rule should now look like the below window:

- Click on the "*add exception*" button once more.

- Under the "Except if" option, select:

- "*A message header*" and "*matches these text patterns*".
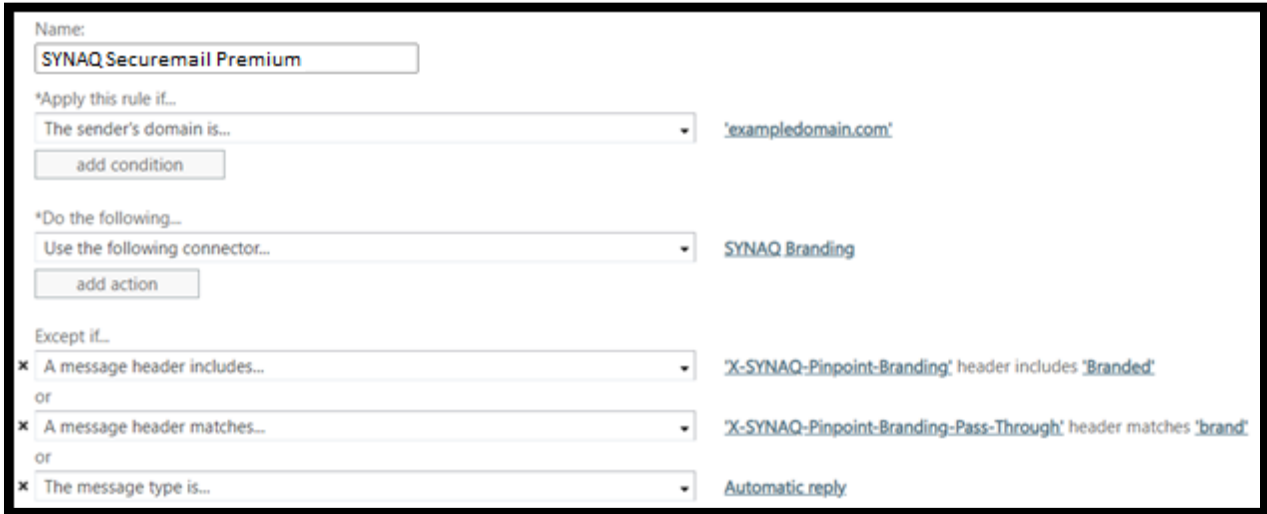

- You will now be required to specify the words by clicking on the "Enter text" and "Enter words" options on the right.

- Under the "Enter text" option, input:
- "X-SYNAQ-Pinpoint-Branding-Pass-Through"
- Under the "Enter words" option, input:
- "brand".

A message header matches... ▾	'X-SYNAQ-Pinpoint-Branding-Pass-Through' header matches 'brand'

- The Transport layer rule will look like the below

Name:

SYNAQ Securemail Premium

*Apply this rule if...

| The sender's domain is... ▾ | 'exampledomain.com' |

add condition

*Do the following...

| Use the following connector... ▾ | SYNAQ Branding |

add action

Except if...

| ✖ | A message header includes... ▾ | 'X-SYNAQ-Pinpoint-Branding' header includes 'Branded' |
or		
✖	A message header matches... ▾	'X-SYNAQ-Pinpoint-Branding-Pass-Through' header matches 'brand'
or		
✖	The message type is... ▾	Automatic reply

- Click "*SAVE*" to save the setup
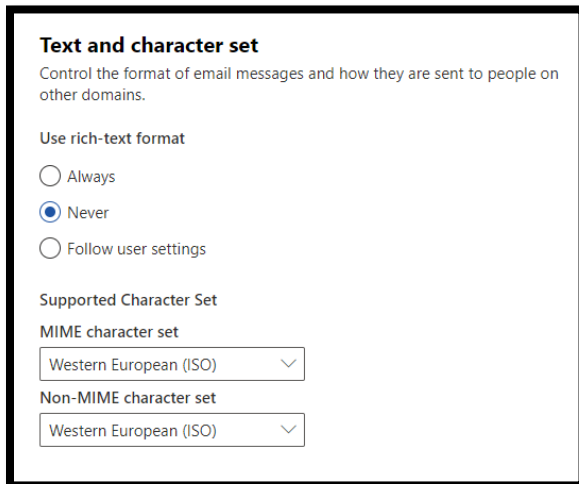
2.4.   Step 4 – Turning Off Rich Text

- Select "remote domains" from the main menu options at the top of the screen.
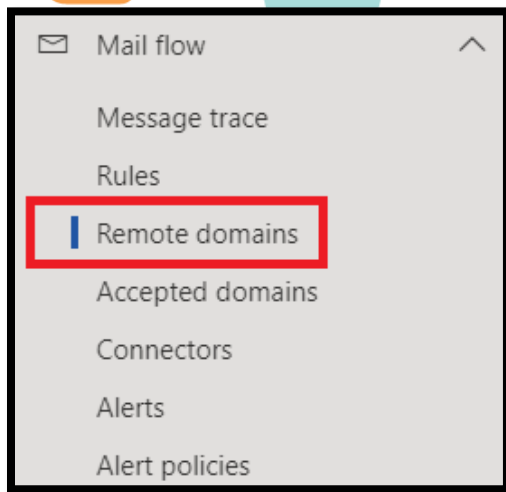
- Edit the default rule clicking on *Edit text and character set*
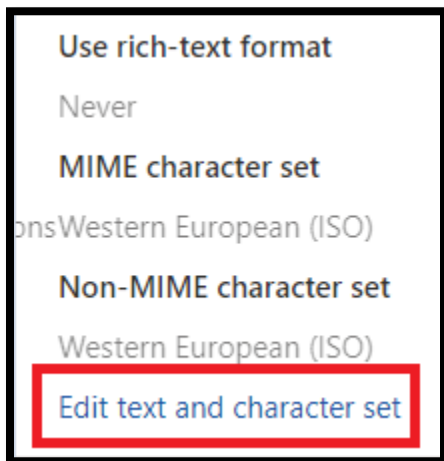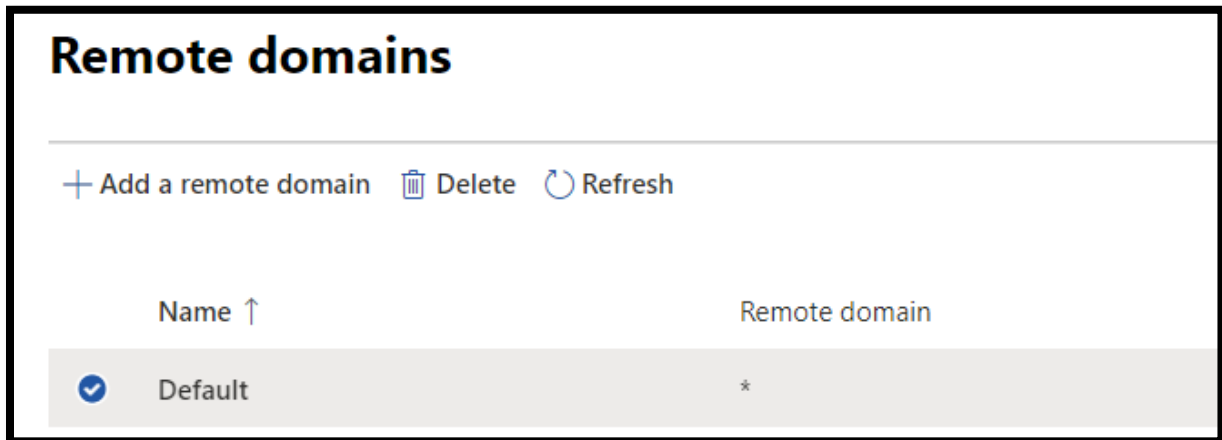
- Under "use rich-text format" select "Never".
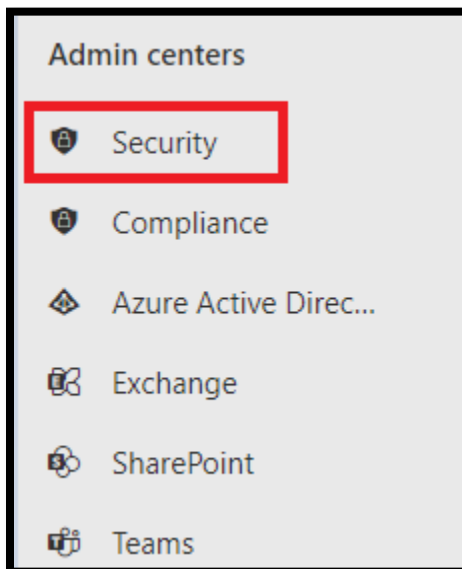

- Lastly, click "Save".

2.5.   Step5 - Allowing SYNAQ IP range through Spam Filter
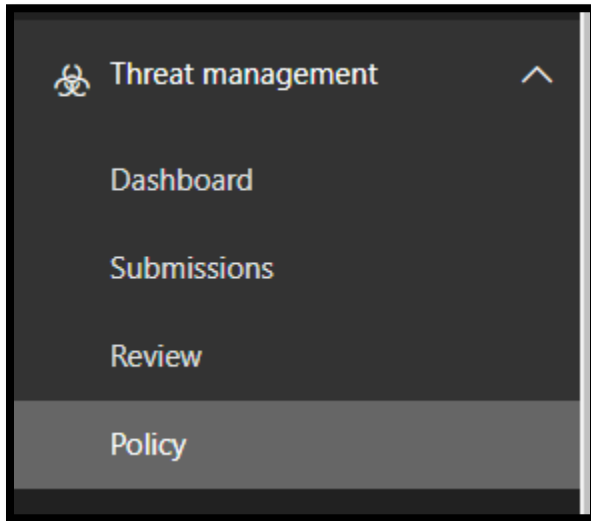
To ensure SYNAQ emails are delivered to your Microsoft 365 mailboxes, you will need to add SYNAQ IPs to your IP Allow List in Exchange Online.

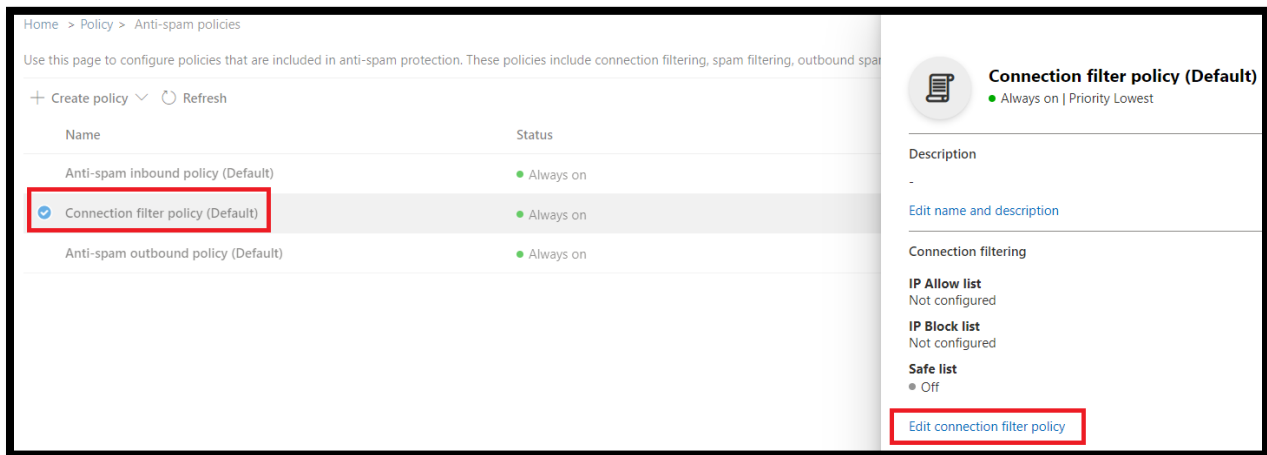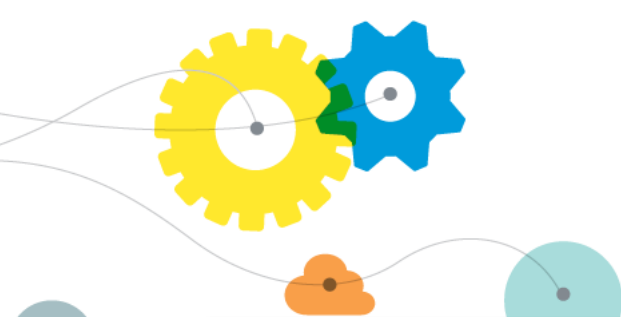1. Open the **Security & Compliance Centre** in Admin Centre

2. Navigate to **Threat management** > **Policy** > **Anti-Spam**

3. On the **Anti-Spam** settings page, expand **Connection filter policy** by clicking the downward arrow

4. Click *Edit Policy*

5. In the **Default** flyout, find **IP Allow List** and click *Edit*

6. In the **Address or address range** box, click *Add +* and enter the iMail IP:

   196.35198.0/24

Connection filter policy (Default)
● Always on | Priority Lowest

Always allow messages from the following IP addresses or address range:

196.35.198.0/24   ✕

Always block messages from the following IP addresses or address range:

☐ Turn on safe list

7. Lastly, click "Save".