iMail Outbound Connector for Office 365 Setup Guide – ver 1.1

1. Purpose

The purpose of this document is to detail how to set-up an SMTP connector on Office 365 to Securemail.

2. iMail Securemail – O365 Set-up

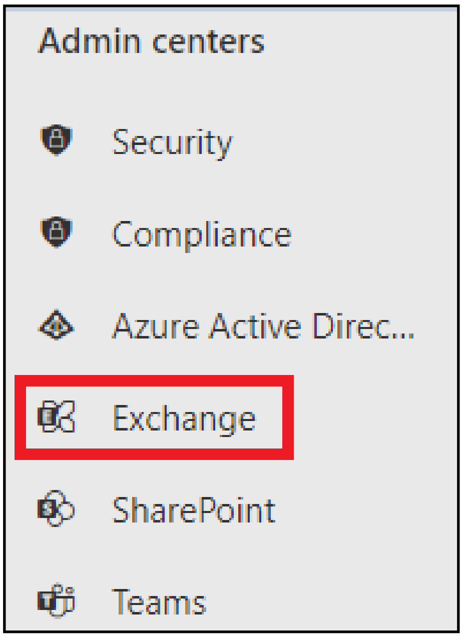
2.1. Step 1 – DNS Changes

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

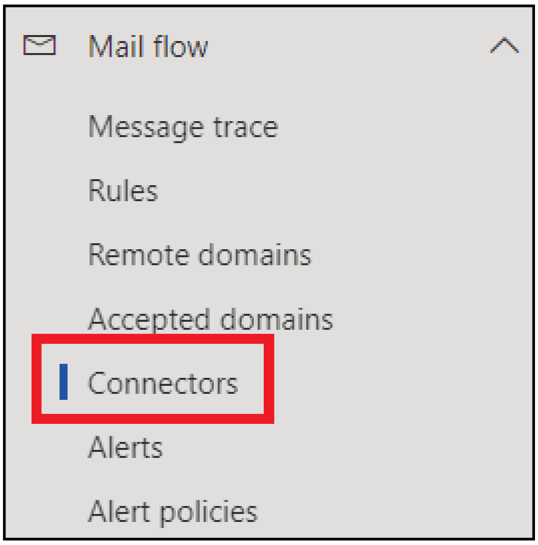
- Add the following entry to your SPF record:
  "v=spf1 include:_spf-securemail.iMail.com -all"

2.2. Step 2 – Configuring the Securemail Connector

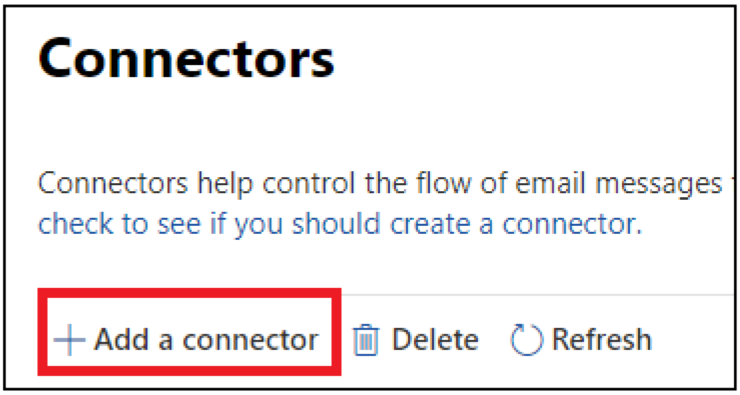
- Login to your O365 portal and click on drop down "*Admin Centers*" on the left-hand side of your screen.



- Click on the "*Mail Flow*" drop down from your menu and click on "*Connectors*"



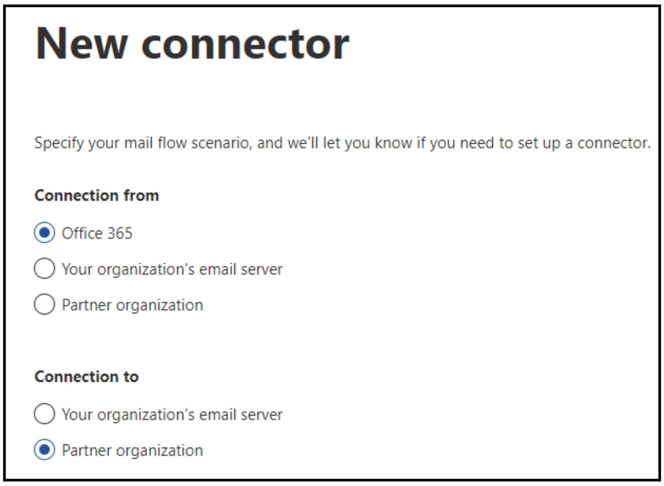
- Click on "*+Add a connector*" sign to create new connector.



Connectors

Connectors help control the flow of email messages
check to see if you should create a 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.

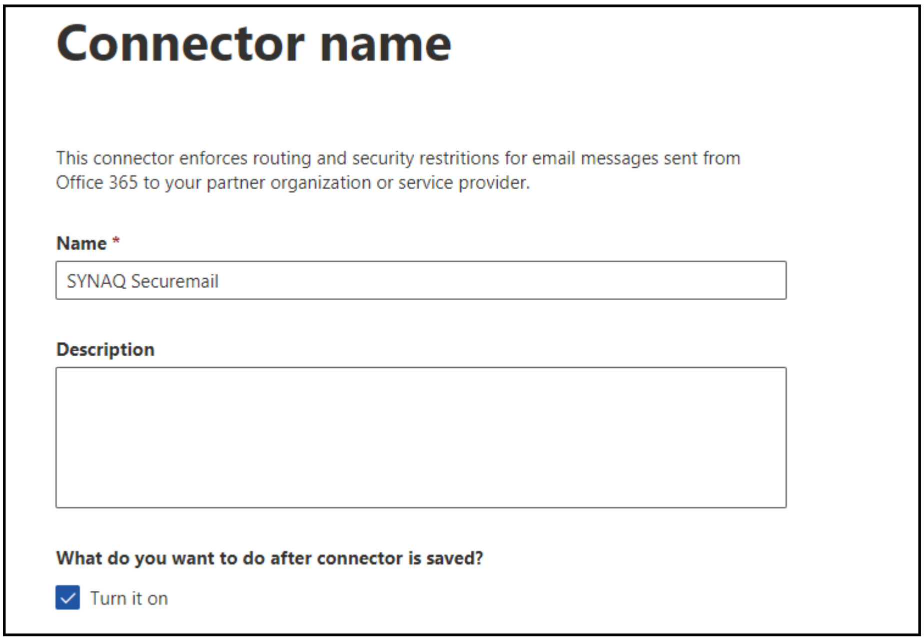
Connection from

● 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 "SYNAQ Securemail" 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 *

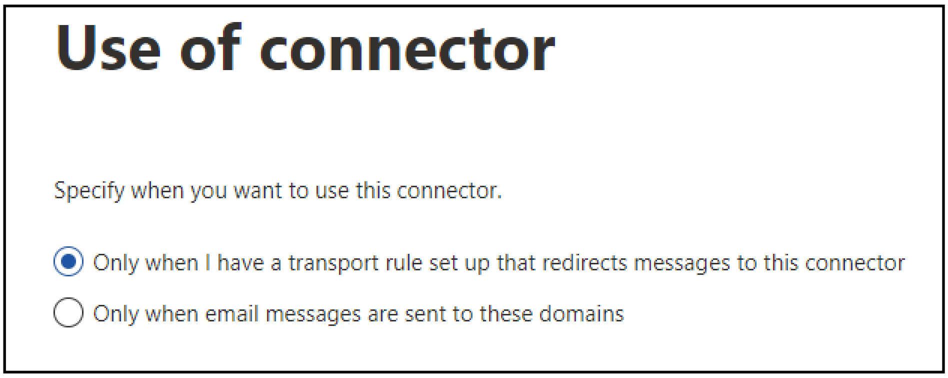
SYNAQ Securemail

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.



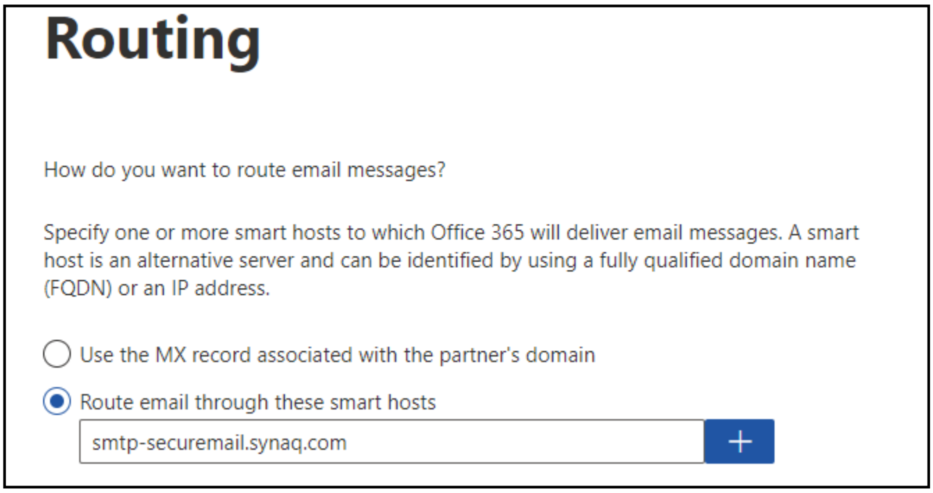
Use of connector

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.iMail.com**



Routing

How do you want to route email messages?

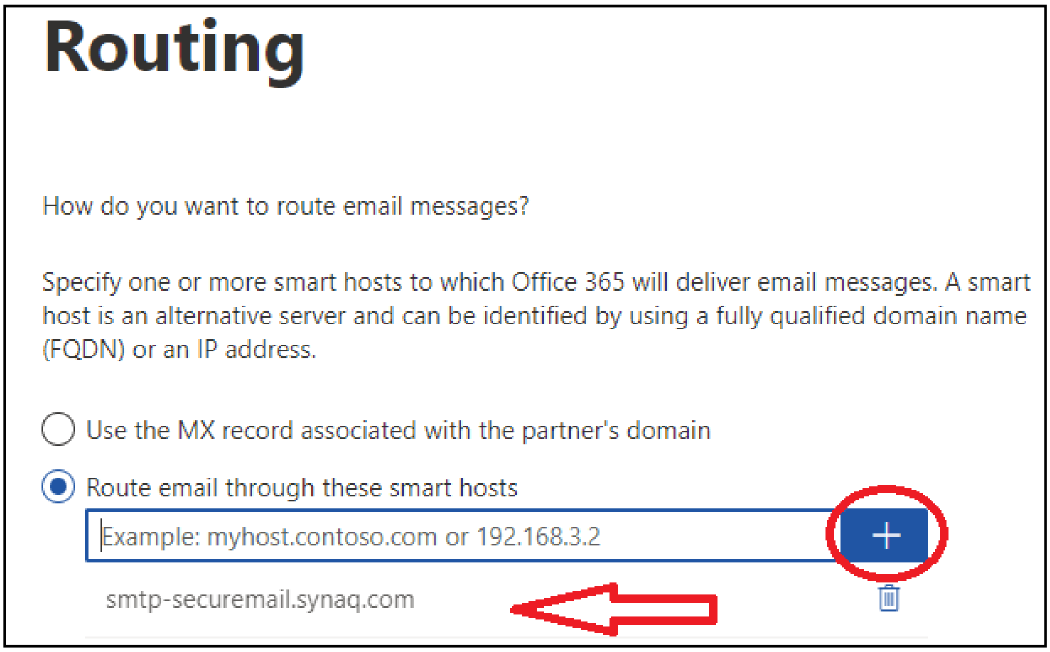
Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address.

○ 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.

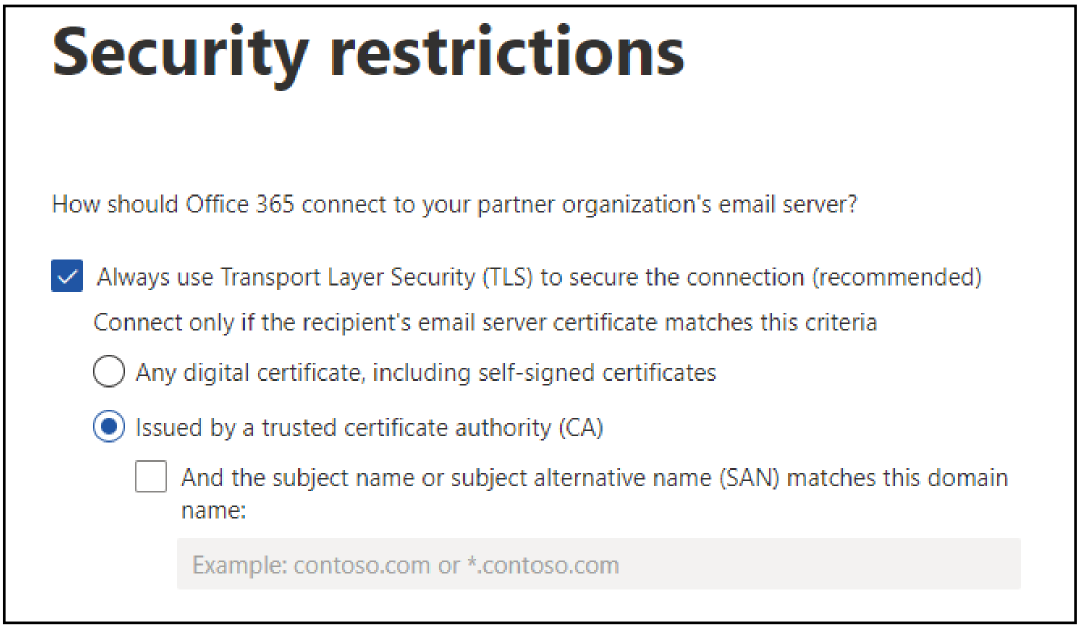
○ Use the MX record associated with the partner's domain

● 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

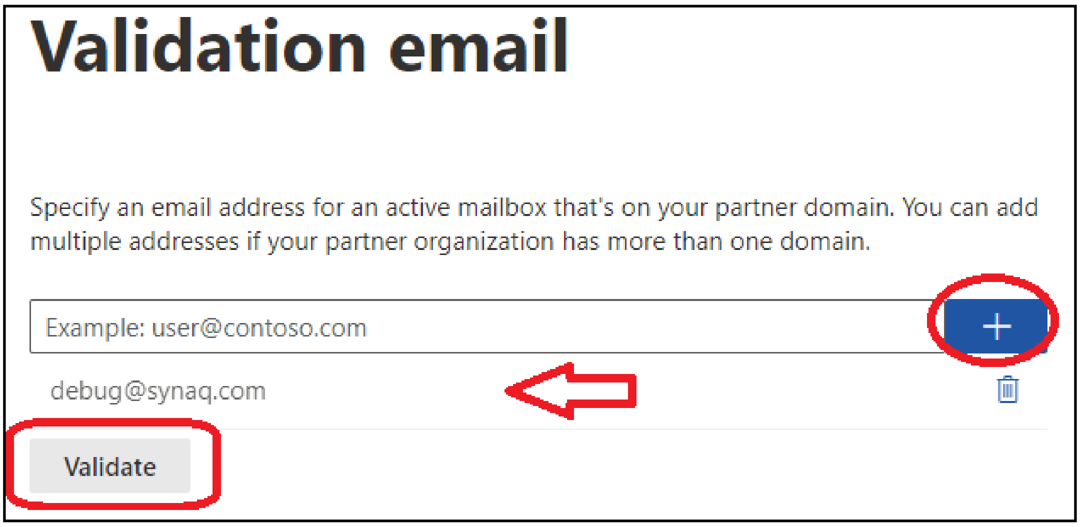
○ Any digital certificate, including self-signed certificates

● 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@iMail.com and;
- Click on the blue plus button to add that email for validation usage.
- Click on “*Validate”* to verify the Connector settings.



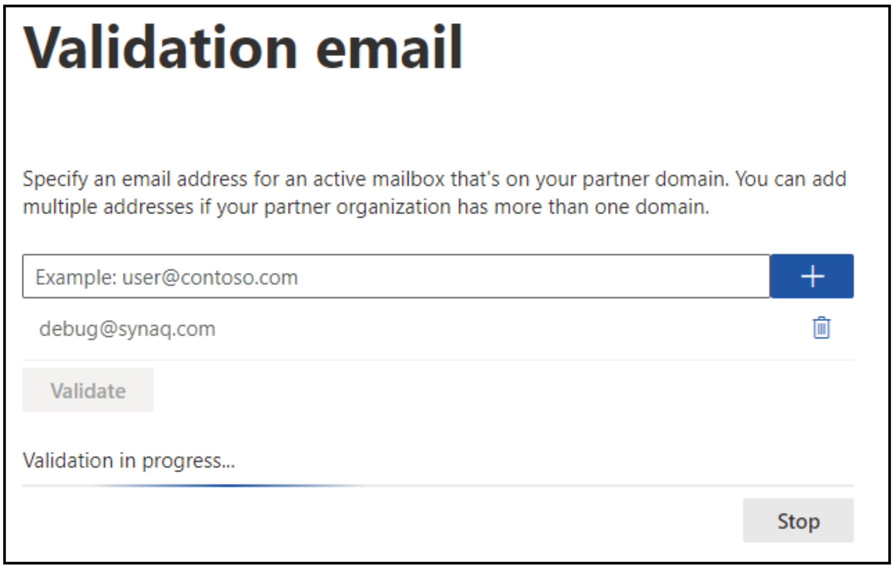
Validation email

Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.

Example: user@contoso.com

debug@synaq.com

- Validation in progress is what you will see next.



Validation email

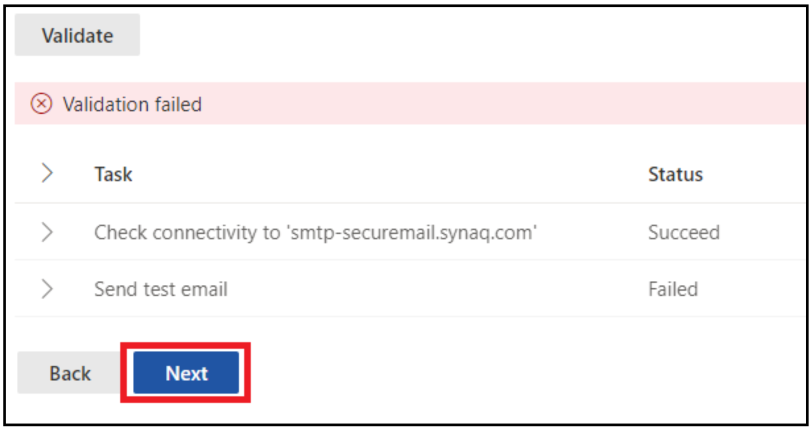
Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.

Example: user@contoso.com

debug@synaq.com

Validation in progress...

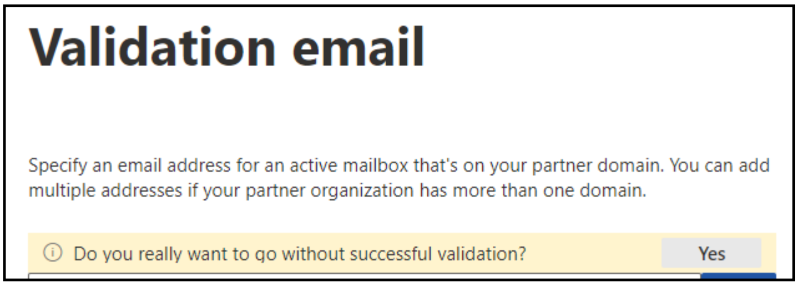
- Please note: even though the validation will fail, this is not a concern and does not cause any issues. Click on “*Next”* to continue.



Validation failed

Task	Status
Check connectivity to 'smtp-securemail.synaq.com'	Succeed
Send test email	Failed

- 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.



Validation email

Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.

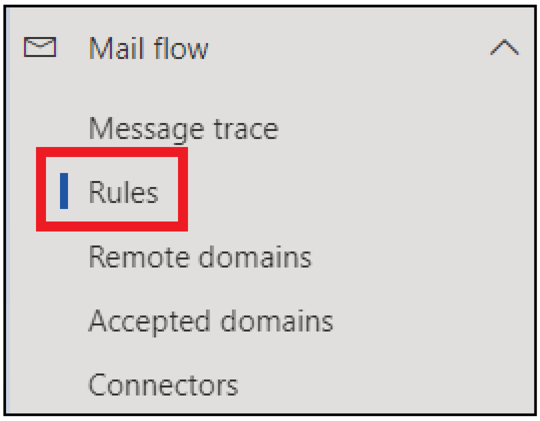
Do you really want to go without successful validation?

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

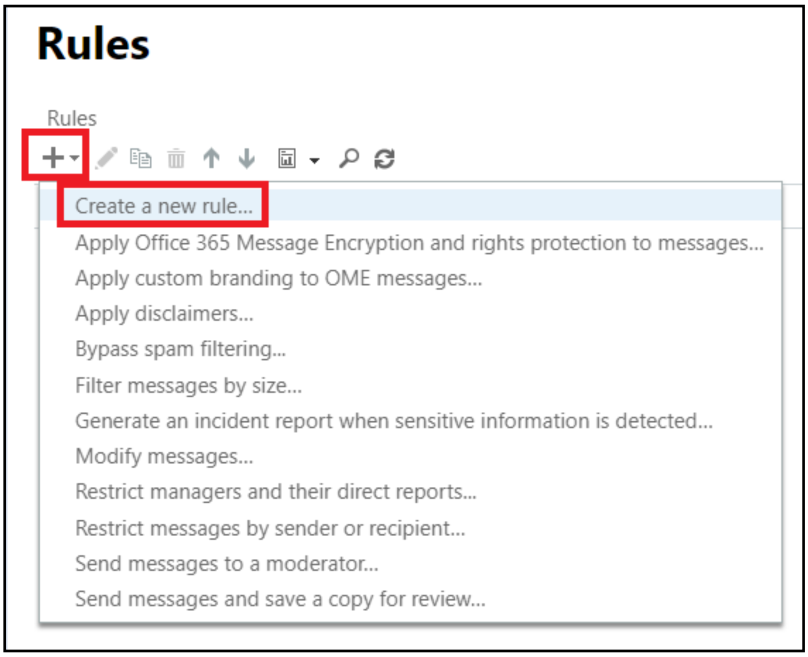
2.3. Step 3 – Creating Securemail Transport Rule

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.

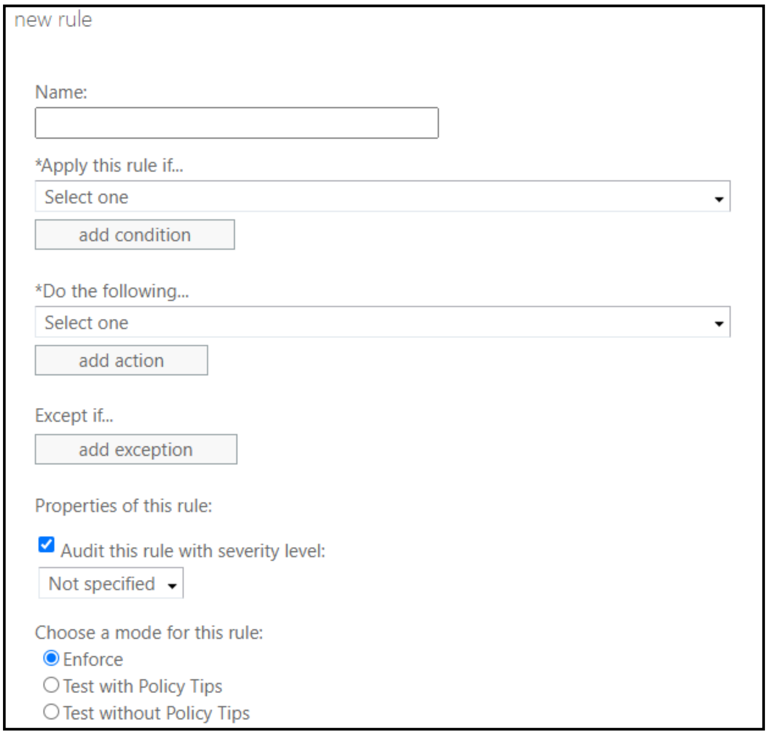
- Select "*Rules*" from the drop-down menu "*Mail Flow*"



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


Rules
Rules
+
Create a new rule...
Apply Office 365 Message Encryption and rights protection to messages...
Apply custom branding to OME messages...
Apply disclaimers...
Bypass spam filtering...
Filter messages by size...
Generate an incident report when sensitive information is detected...
Modify messages...
Restrict managers and their direct reports...
Restrict messages by sender or recipient...
Send messages to a moderator...
Send messages and save a copy for review...

- 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).



new rule

Name:

*Apply this rule if...

Select one

add condition

*Do the following...

Select one

add action

Except if...

add exception

Properties of this rule:

☑ Audit this rule with severity level:

Not specified

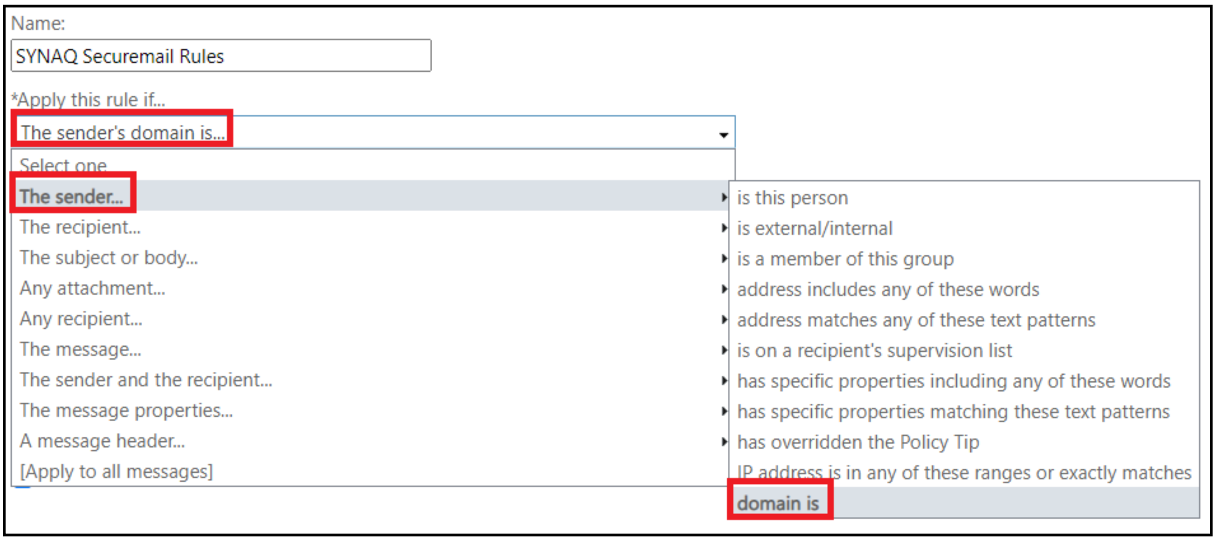
Choose a mode for this rule:

● Enforce

○ Test with Policy Tips

○ Test without Policy Tips

- Input/select the following information:
  - Name**:** Input “iMail Securemail Rules”
  - Apply this rule if: Select “The sender” and “domain is”



Name:

SYNAQ Securemail Rules

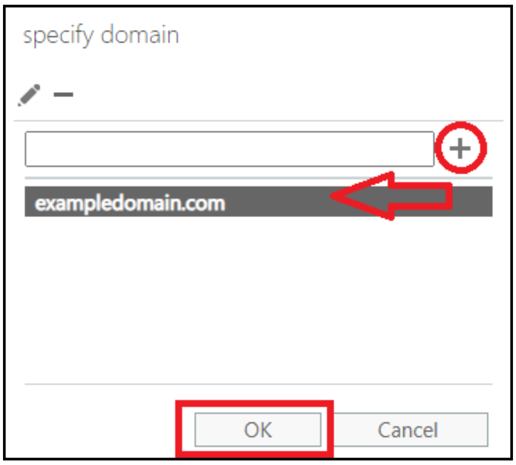
*Apply this rule if...

The sender's domain is...

Select one
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...
[Apply to all messages]
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
domain is

- This will prompt a new window requesting you to “*specify domain*”.

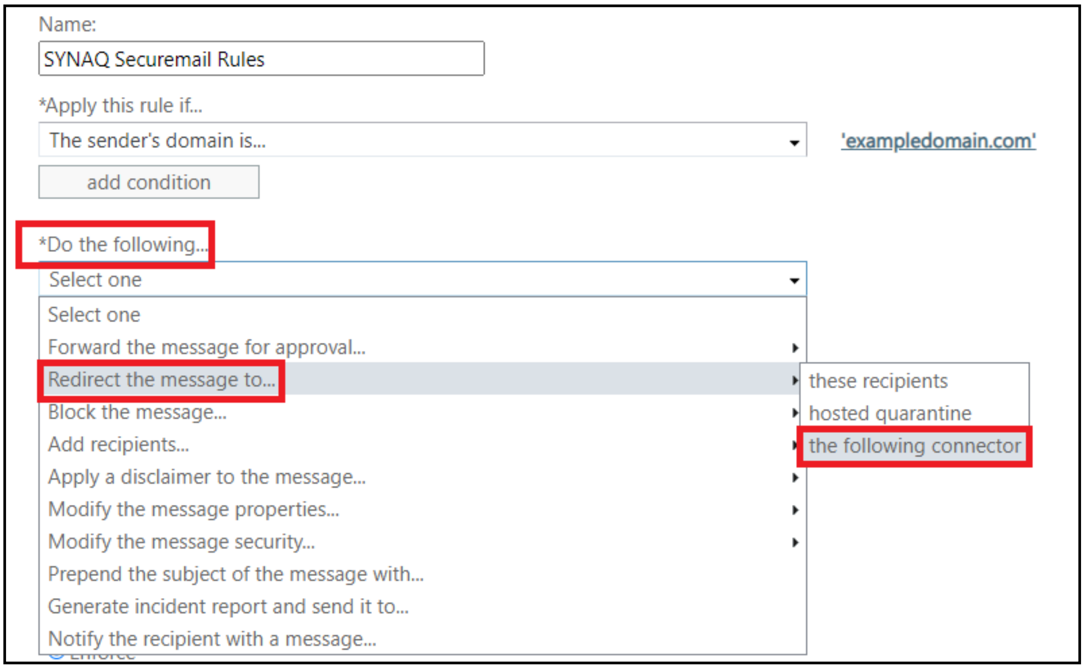
- Input your own company domain, that require the mail to be routed to the Send Connector.
- Click the "+" sign and then click "*Ok*".



specify domain

exampledomain.com

- Under the "Do the following" option, select "*redirect the messages to*" and select "*the following connector*".



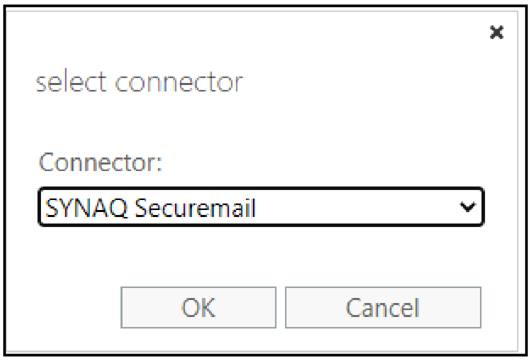
Name:
SYNAQ Securemail Rules

*Apply this rule if...
The sender's domain is... 'exampledomain.com'

*Do the following...
Select one

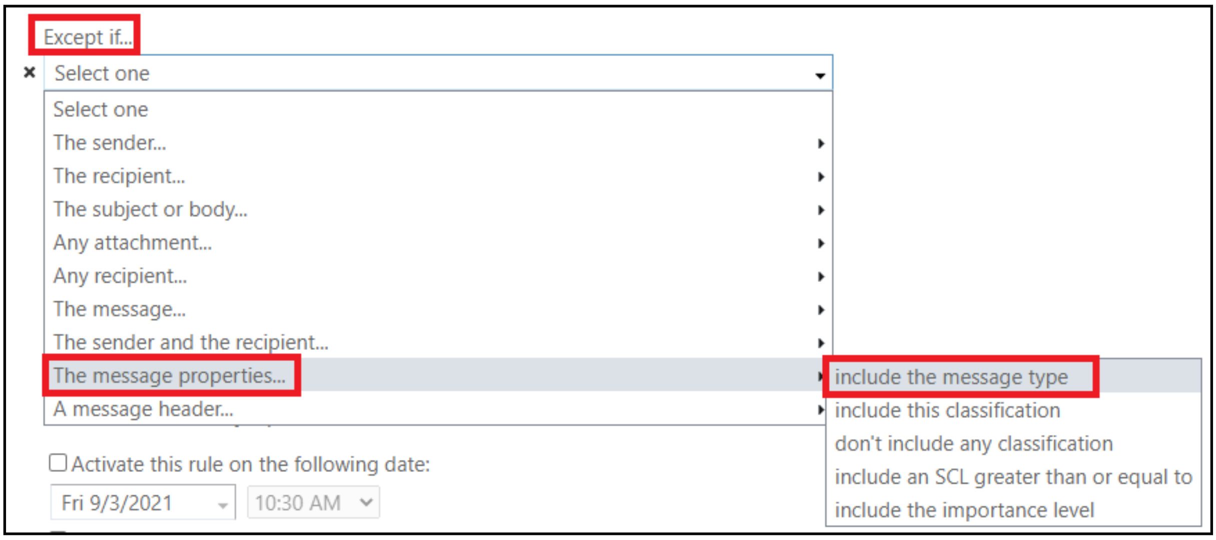
add condition
Select one
Forward the message for approval...
Redirect the message to...
Block the message...
Add recipients...
Apply a disclaimer to the message...
Modify the message properties...
Modify the message security...
Prepend the subject of the message with...
Generate incident report and send it to...
Notify the recipient with a message...
these recipients
hosted quarantine
the following connector

- Select the "*SYNAQ Securemail*" Connector.


select connector

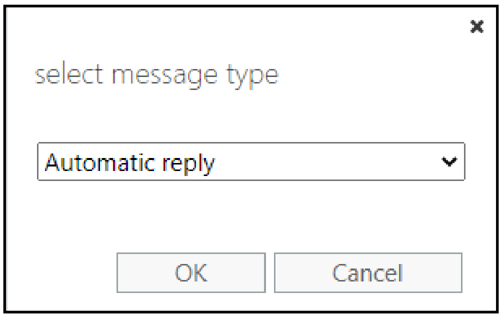
Connector: SYNAQ Securemail

- We will need to add an "*Exception*" to bypass automatic replies from being sent through the Connector.
- Click *"Add Exception"* and choose options *"The Message Properties" -> "Include the Message Type".*


Except if...
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...
A message header...
include the message type
include this classification
don't include any classification
include an SCL greater than or equal to
include the importance level

☐ Activate this rule on the following date: Fri 9/3/2021 10:30 AM

- Choose from the list *"Automatic Reply"* and click on *"Ok*".

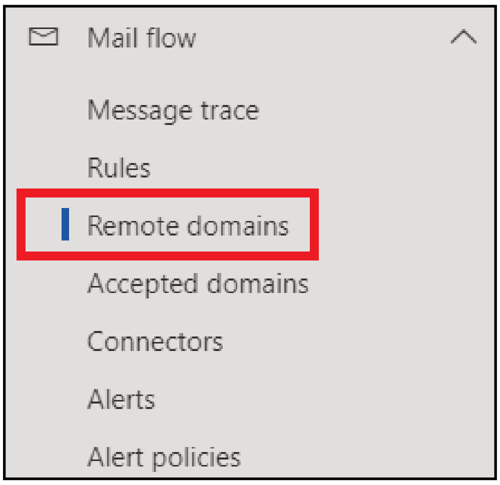

select message type

Automatic reply

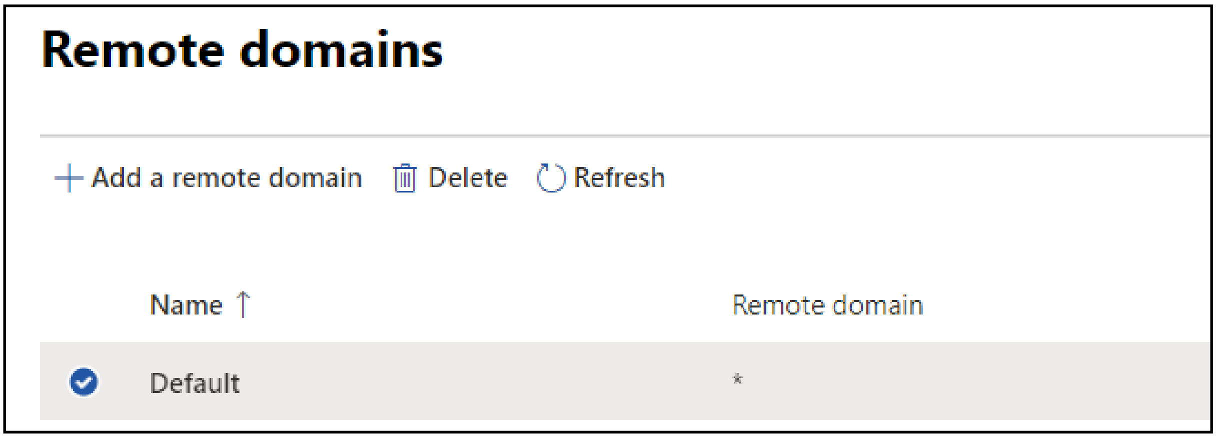
- At the bottom of the page, click on *"Save"* to complete the setup of the rules.

2.4. Step 4 – Turning Off Rich Text

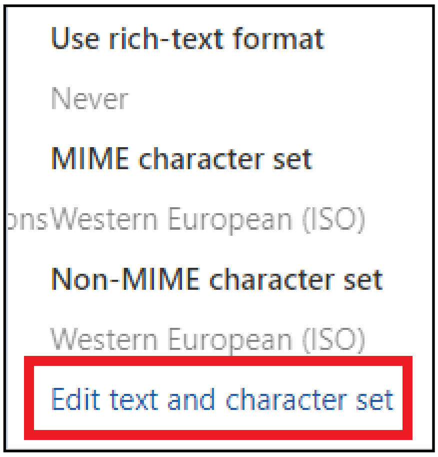
- Select “remote domains” from the main menu options at the top of the screen.



- Edit the default rule clicking on “*Edit text and character set”.*


Remote domains

Name ↑	Remote domain
Default	*


Use rich-text format

Never

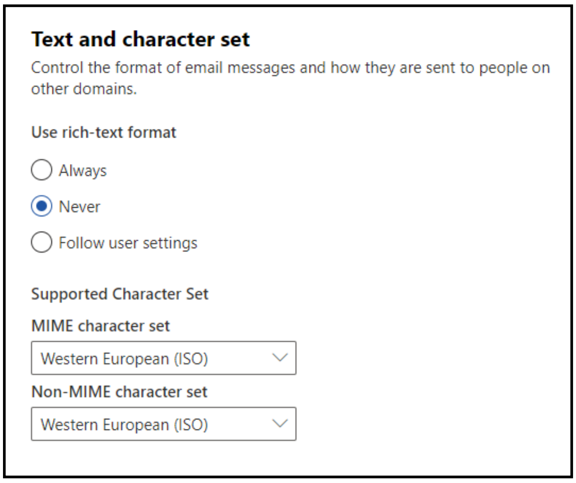
MIME character set

onsWestern European (ISO)

Non-MIME character set

Western European (ISO)

- Under “use rich-text format” select “*Never*”.



Text and character set

Control the format of email messages and how they are sent to people on other domains.

Use rich-text format

○ Always

● Never

○ Follow user settings

Supported Character Set

MIME character set

Western European (ISO)

Non-MIME character set

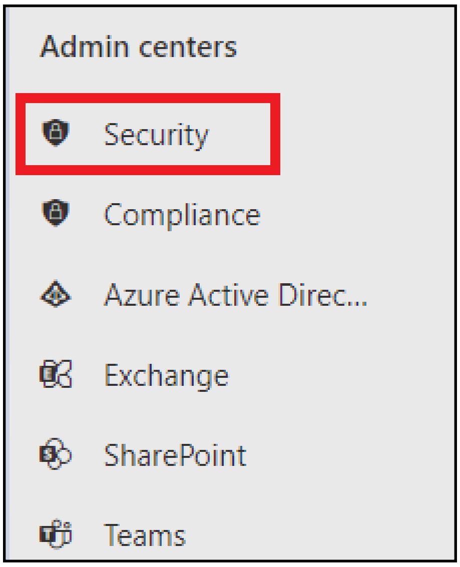
Western European (ISO)

- Lastly, click “*Save*”.

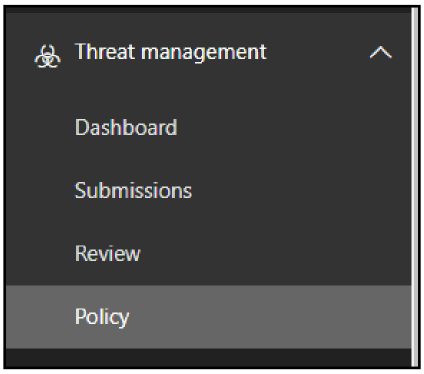
2.5. Allowing iMail IP range through Spam Filter

To ensure iMail emails are delivered to your Microsoft 365 mailboxes, you will need to add iMail IPs to your IP Allow List in Exchange Online.

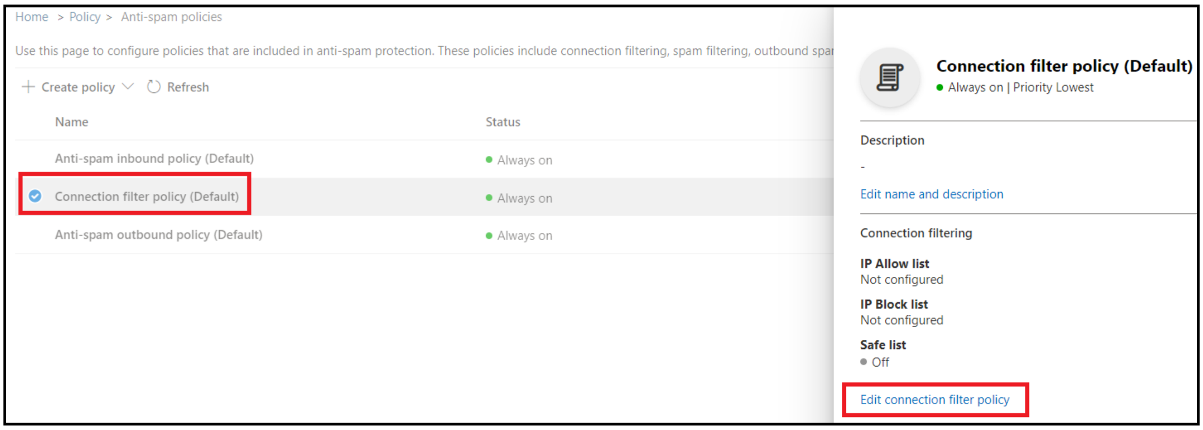
- Open the **Security & Compliance Centre** in Admin Centre.



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



- On the **Anti-Spam** settings page, expand **Connection filter policy** by clicking the downward arrow.
- Click *“Edit Policy”.*


Home > Policy > Anti-spam policies
Create policy
Refresh
Edit name and description
Edit connection filter policy

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, outbound spa

Name	Status
Anti-spam inbound policy (Default)	● Always on
Connection filter policy (Default)	● Always on
Anti-spam outbound policy (Default)	● Always on

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

Description
-

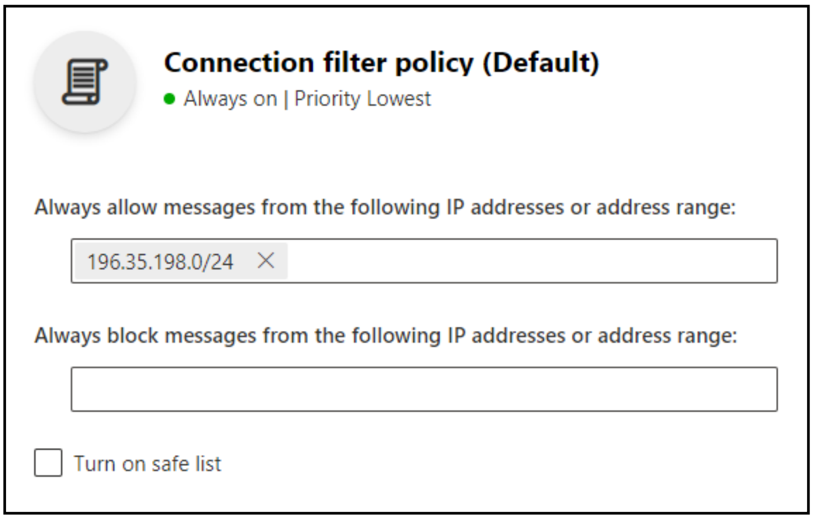
Connection filtering

IP Allow list
Not configured

IP Block list
Not configured

Safe list
● Off

- In the **Default** flyout, find **IP Allow List** and click *“Edit”.*
- In the **Address or address range** box, click *“Add +”* and enter the iMail IP: 196.35198.0/24
- Click “*Save*”.



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