COMODO
Creating Trust Online®

Office 365 Integration Guide

Software Version 6.7

Guide Version 6.7.050720

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction

Office 365 is Microsoft's cloud solution for accessing email, calendar, and Microsoft office tools. Office 365 allows organizations to host their entire email architecture at an off-site location, and allows Microsoft to manage all the day-to-day aspects of your organization's email.

Comodo Korumail is a cloud-based secure email gateway. It is designed to eliminate spam and email borne malware for customers using cloud-hosted or on-premise mail servers.

This guide contains step-by-step instructions on how to integrate Office 365 with Comodo Korumail. The guide assumes you have a functioning Office 365 deployment.

Advantages of Integrating Korumail and Office 365

Moving your mail to a cloud solution like Office 365 brings a wide range of advantages and flexibility to an organization. Integrating your deployment with Korumail will add the critical, enterprise-grade security required by such a cloud-deployment.

Comodo Korumail protects against targeted invasions using enhanced social engineering attack protection, web reputation, and detection engines. It also employs cloud-based threat analysis to block highly-targeted email attacks by using exploit detection and Comodo patented containment (sandboxing) technology. Integration of these components enables you to defend against advanced malware and targeted attacks.

Auto-containment

Comodo's patented containment technology protects against malicious attachments without sacrificing user productivity. When an attachment is opened, it runs in the Comodo container while the file is analyzed to determine whether or not it's safe. The file cannot access the host's resources or user data while it is in the container, so it can't damage or infect the endpoint.

Comodo Reputation Network

Comodo's comprehensive and highly accurate IP reputation system helps block malicious URLs embedded in emails.

Intelligent filtering

Comodo Korumail uses a sophisticated array of spam filters, anti-virus scanners and content analysis engines to prevent unsolicited mail from ever entering your network. Featuring full integration with the Comodo Valkyrie file verdict system, it delivers true enterprise-level security to cloud-based mail servers.

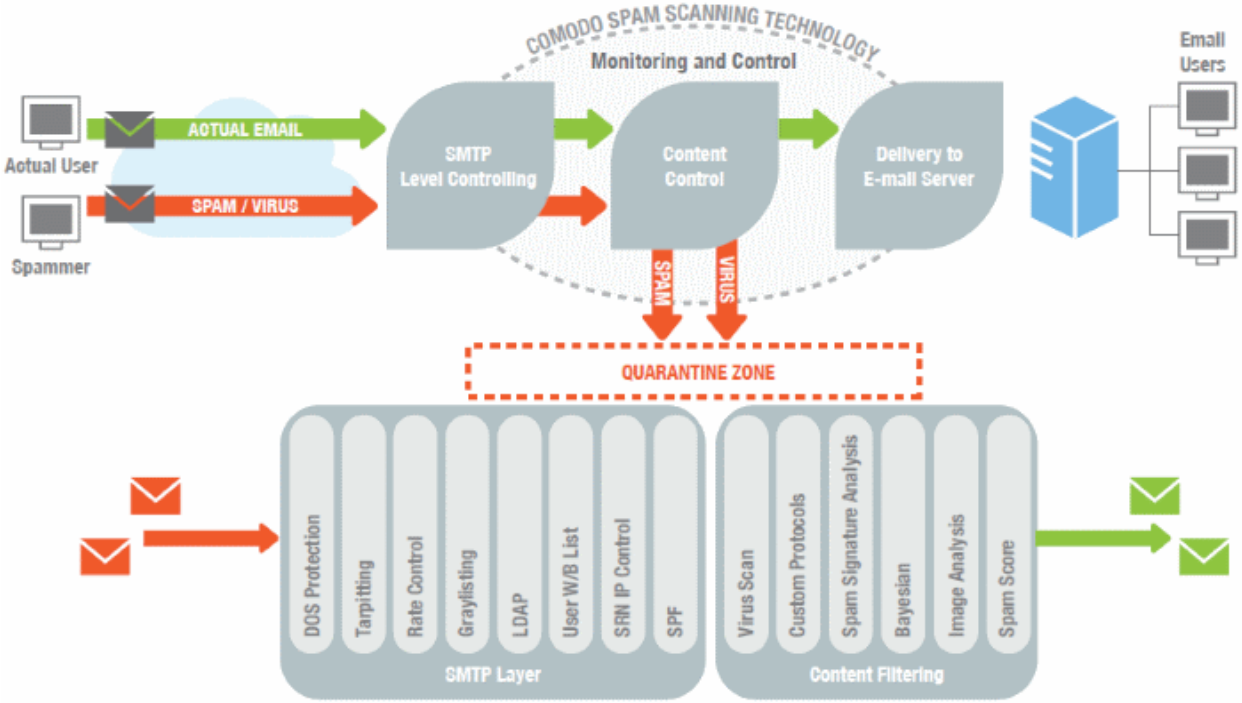
Ease of use

Advanced search options-including search on users or text in sender, receiver, subject, and other fields-make it easy to find emails in the archive. As with quarantined emails, you can take action on archived messages.

Adding Korumail on top of Microsoft Office 365 offers enhanced security, especially with spear-phishing and targeted attack protection, providing you with an additional layer of security against advanced malware and zero-day exploits.

1.1 Email Flow Explanation

In order to better understand how Korumail works in conjunction with Microsoft Office 365, the path the email message takes must first be understood.



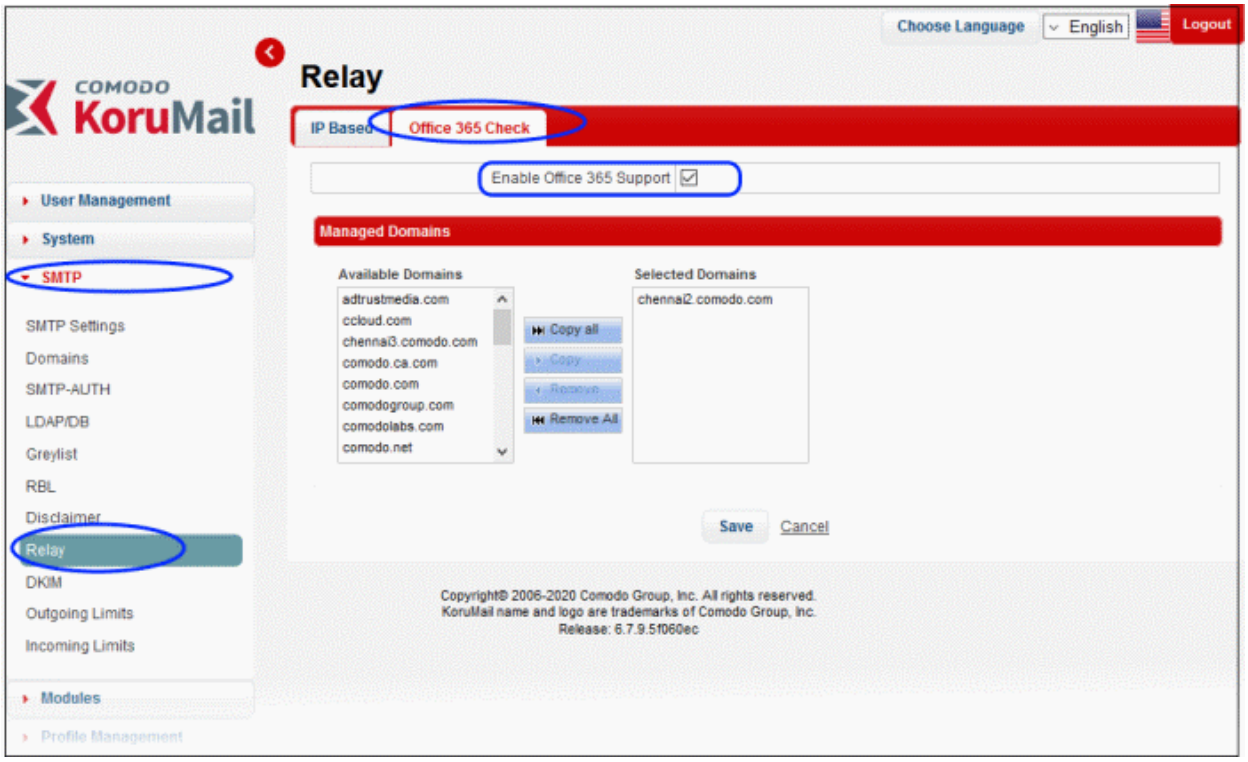
- An email is sent from one organization to the other. For example, an email from someone at senderdomain.com is sent to someone at recipientdomain.com.
- The sender's mail server will look up the MX record of recipientdomain.com. This record will contain the domain name or IP address of the first hop in recipientdomain.com's email architecture. This first hop is the first level of inspection that recipientdomain.com wants performed on their email.
- Since recipientdomain.com is using Comodo Korumail, this will be the first hop for the inbound email.
- Comodo Korumail then inspects the email for spam, phishing attacks, viruses and spyware.
- If the email passes these checks it is sent to recipientdomain.com's next hop, which is their Microsoft Office 365 cloud email server.
- After further processing by Microsoft Office 365, the email is then sent to the recipient's mailbox.

2 Configure Comodo Korumail Settings

Office 365 check on Korumail

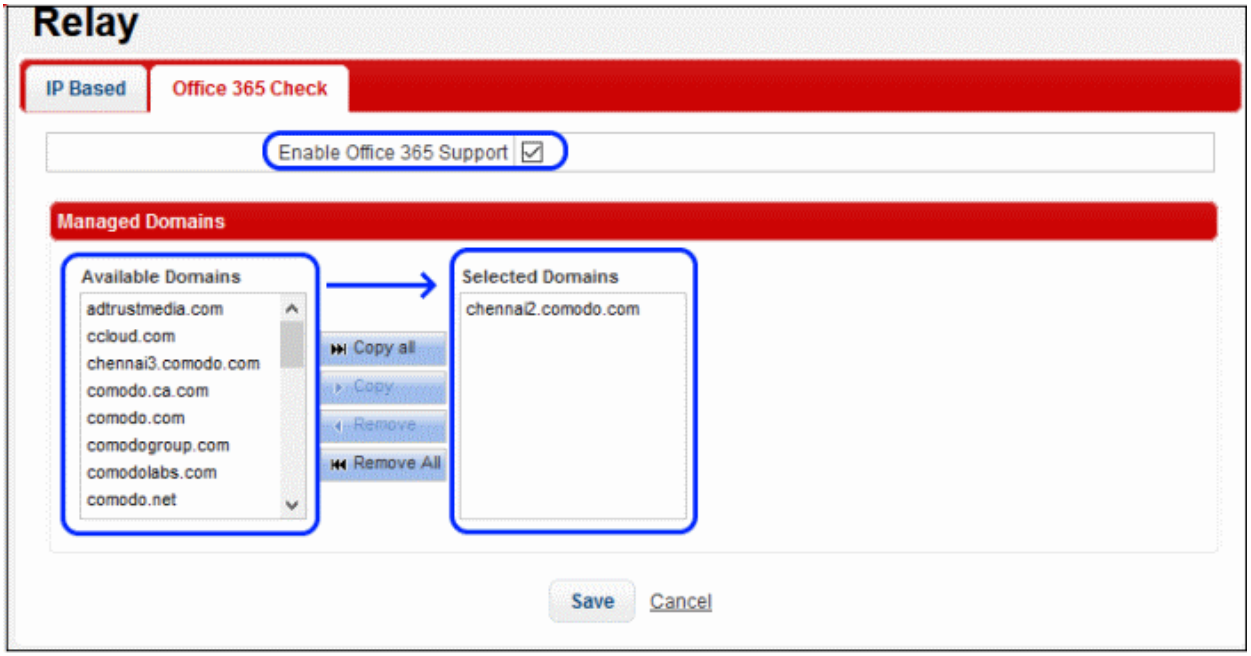
Configure the inbound settings in Comodo Korumail to route emails sent to your domain to Office 365.

1. Log in to your Korumail account
2. Select 'SMTP' in the left menu then click 'Relay'



3. Click 'Office 365 Check':

4. Configure 'Office 365 Check' with the following options:
   i. Enable 'Office 365 Support'
   ii. Select and copy the managed domain names of your Office 365 server from the left list to the right:



- Click 'Save'

Note: You do not need to enter any Office 365 IP or MX records as Comodo Korumail automatically collects the routes in the background.

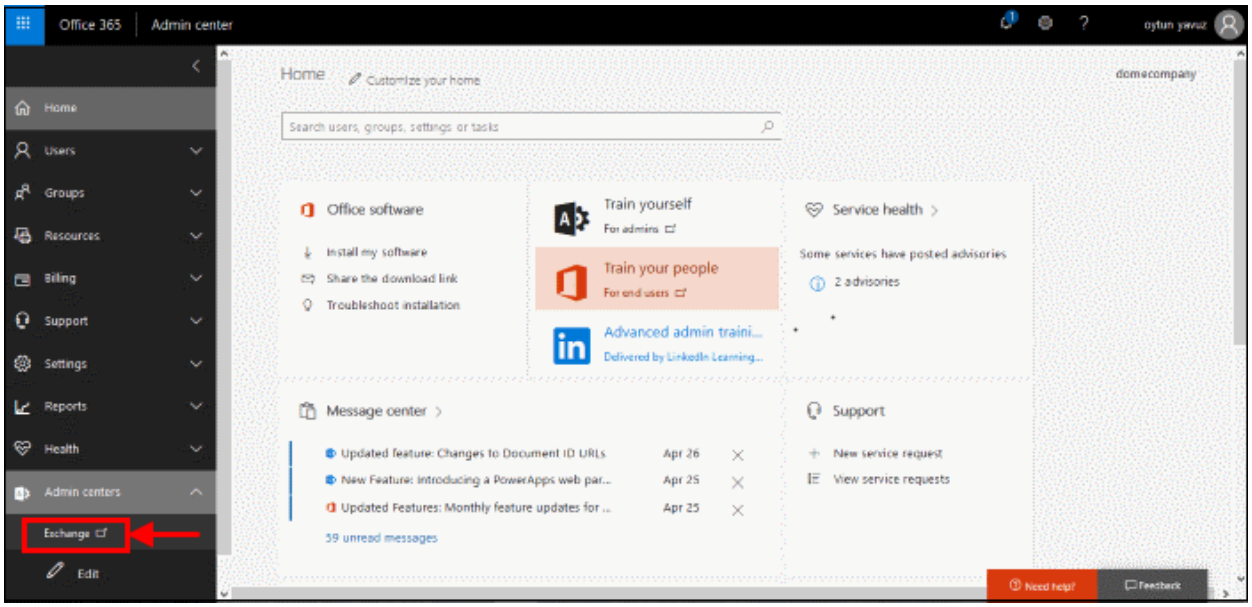
3 Configure Office 365 Settings

The configuration has two email flows:

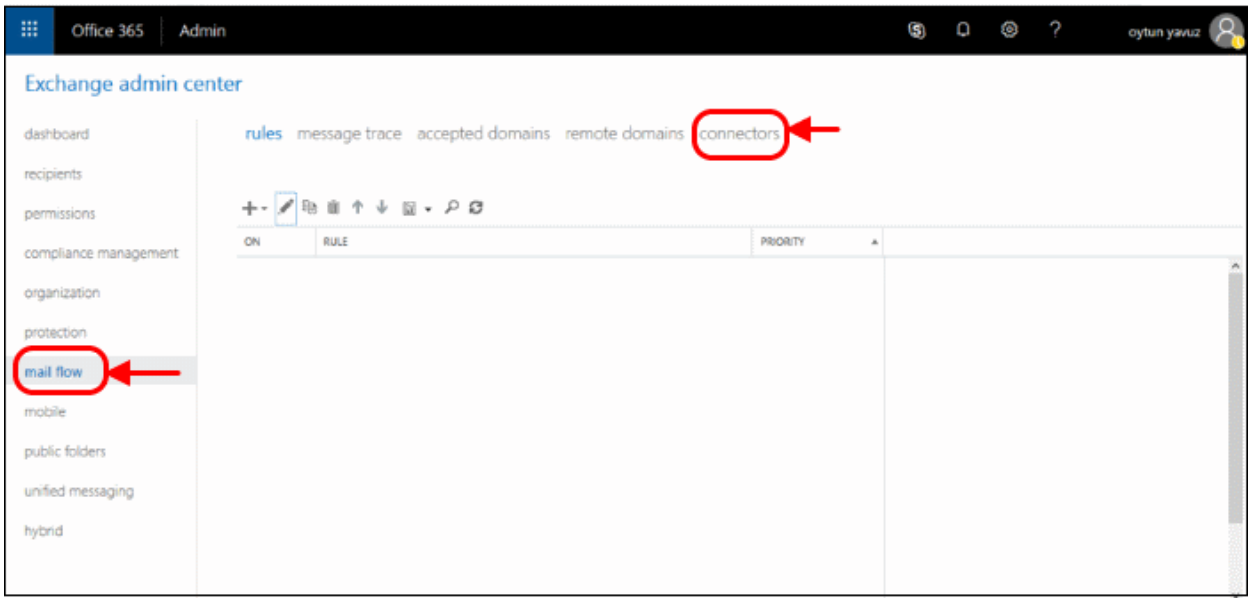
- **Inbound flow setup on Office 365**
- **Outbound flow setup on Office 365**

3.1 Inbound flow setup on Office 365

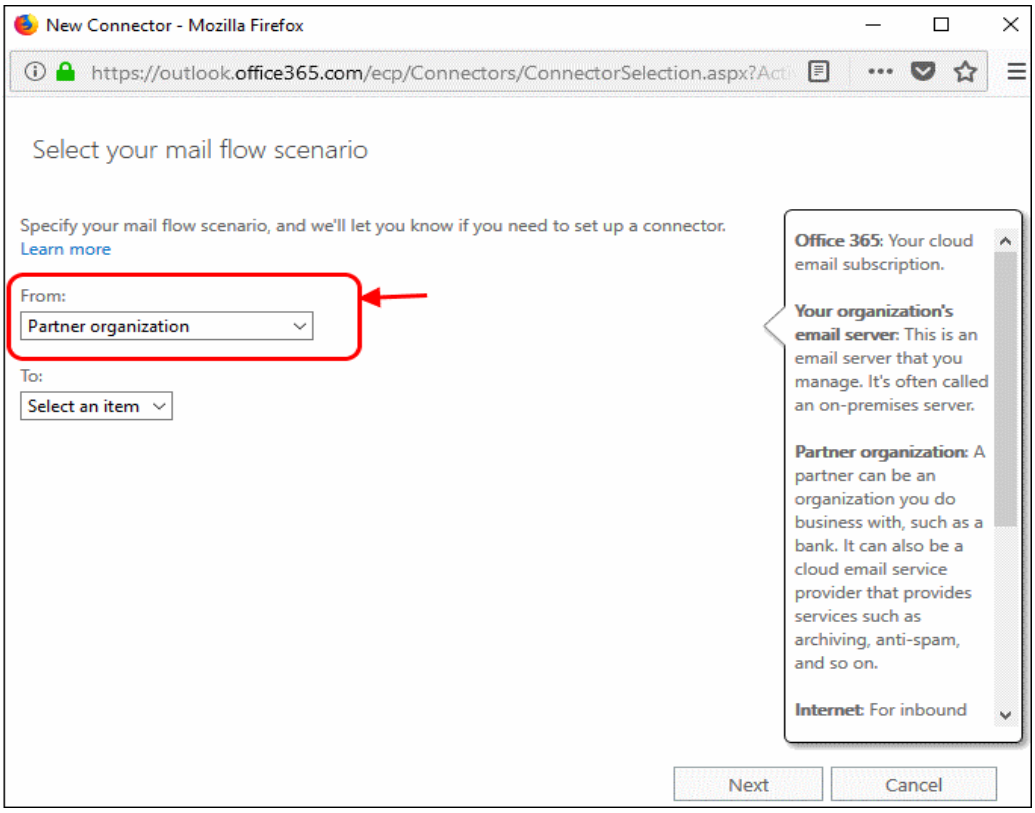
- Log in to your Microsoft Office 365 administrator center account
  - Click 'Admin' in the menu on the left
  - Click 'Admin Centers' > 'Exchange'



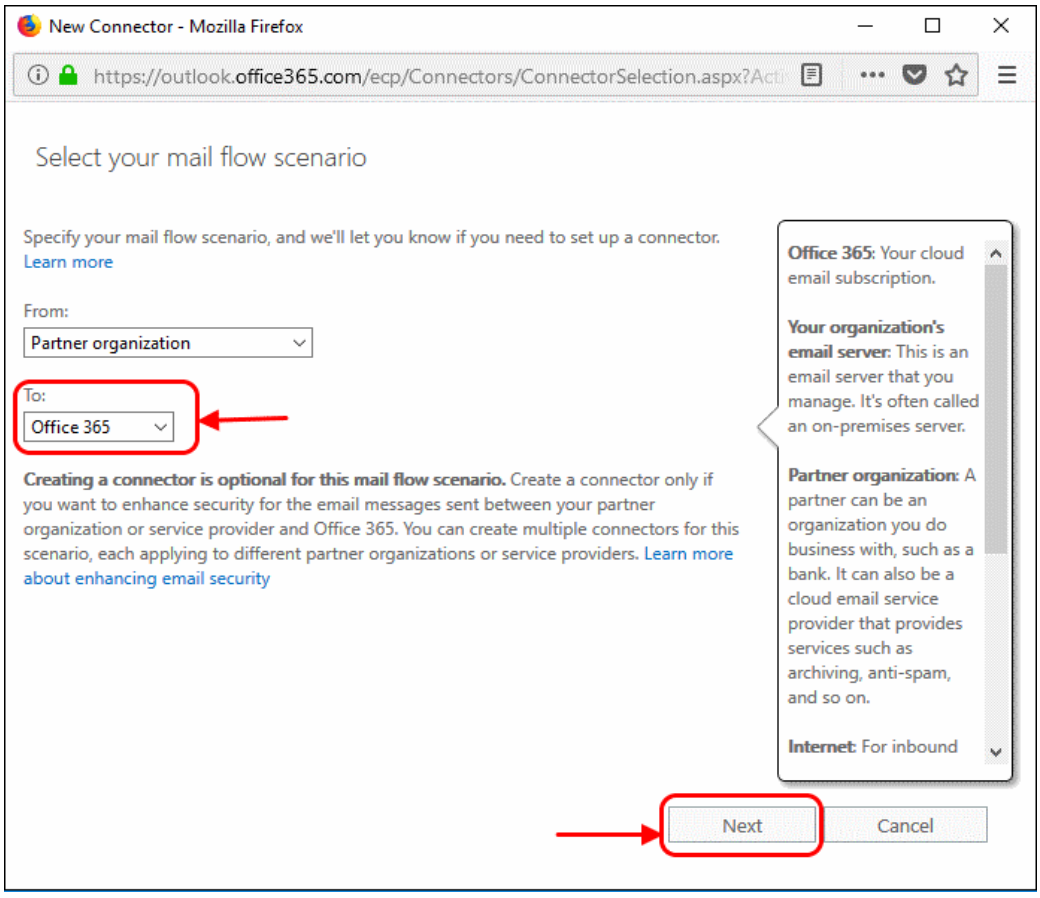
- Click 'Mail Flow' on the left
- Click 'Connectors' in the top navigation:



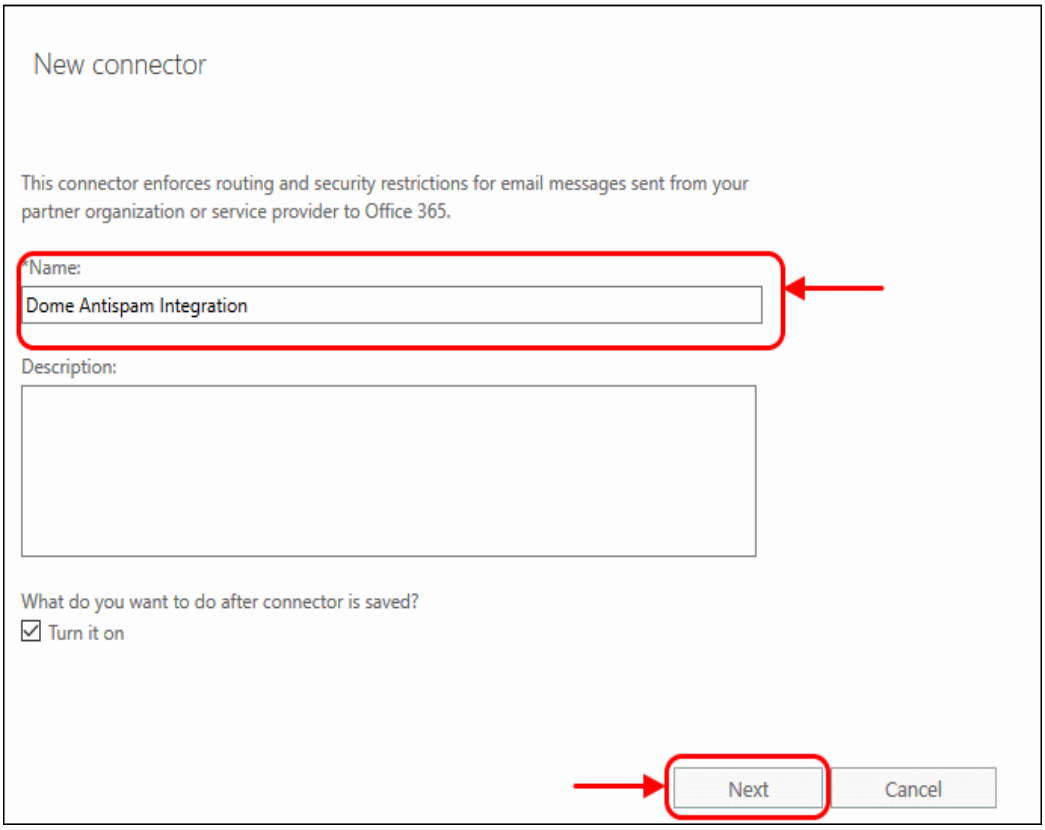
- Add an Inbound Connector.
  - Select 'Partner Organization' in the 'From' drop-down menu



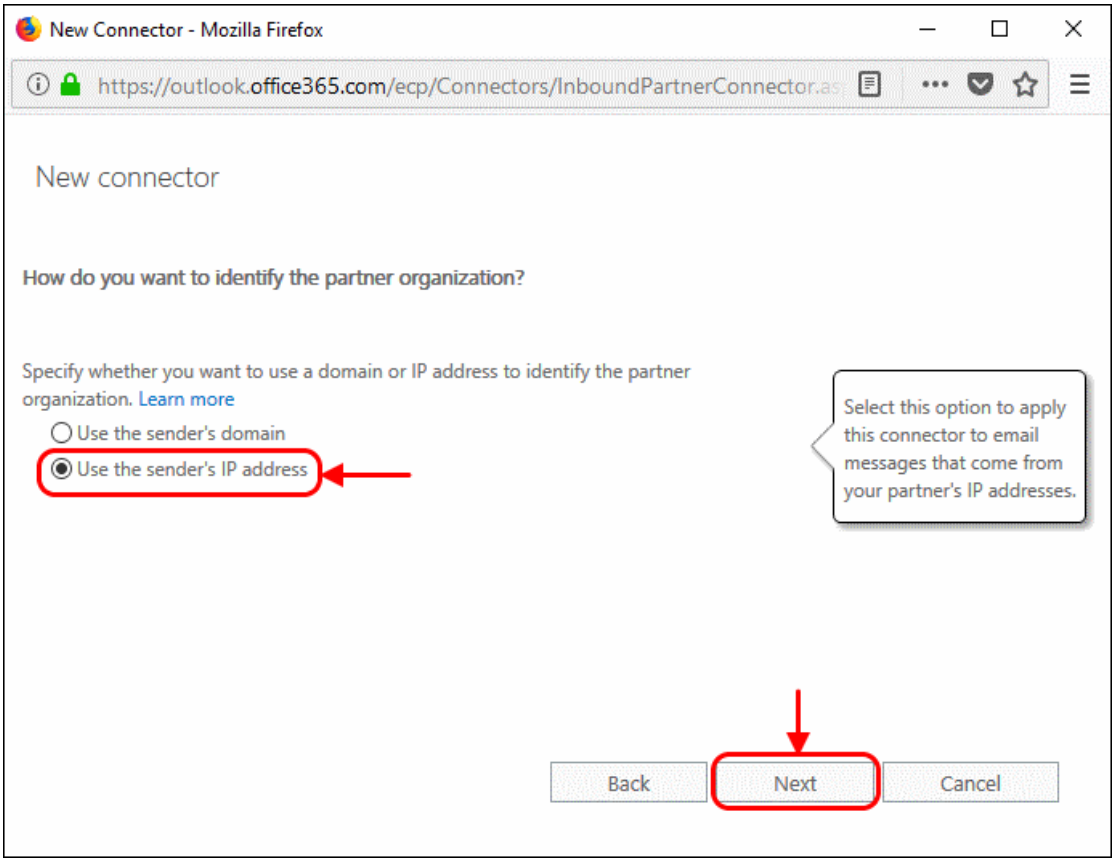
- Select 'Office 365' in the 'To' drop-down
- Click 'Next'



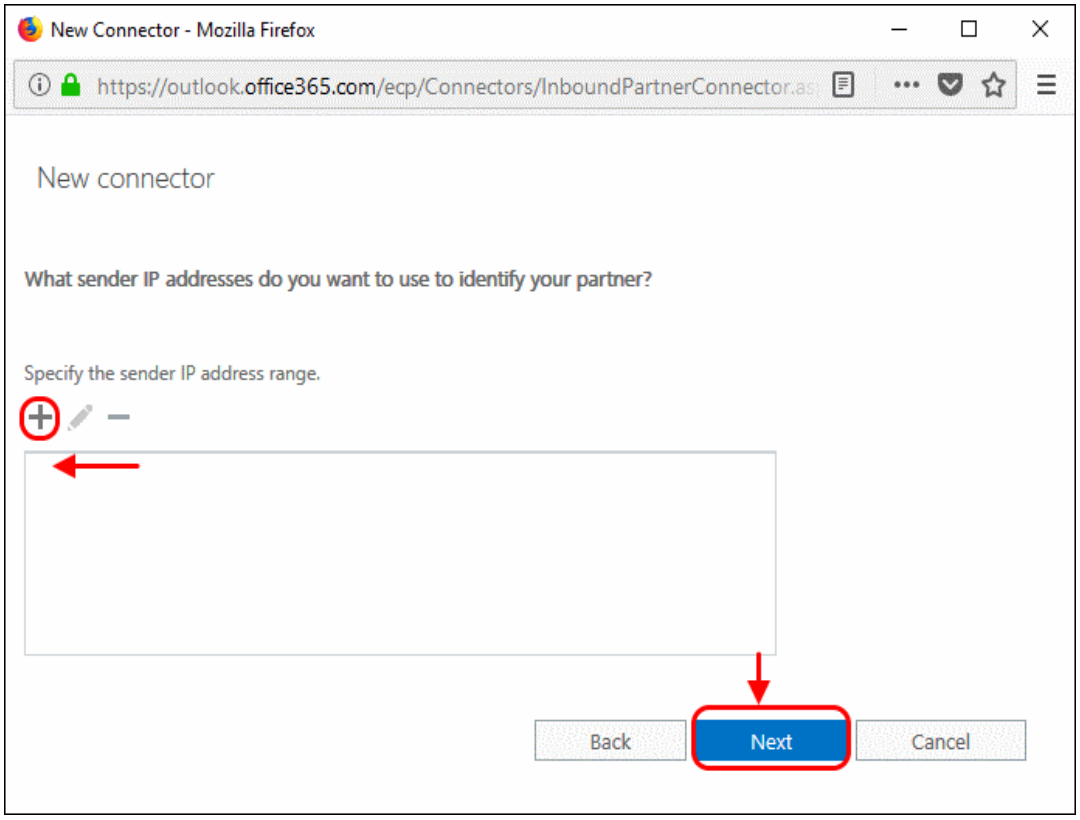
- Enter a descriptive name for the connector in the 'Name' field:
  - Click 'Next':



- Select 'Use the sender's IP address':



- Specify the sender IP addresses range:
  - Click '+' to add new connector

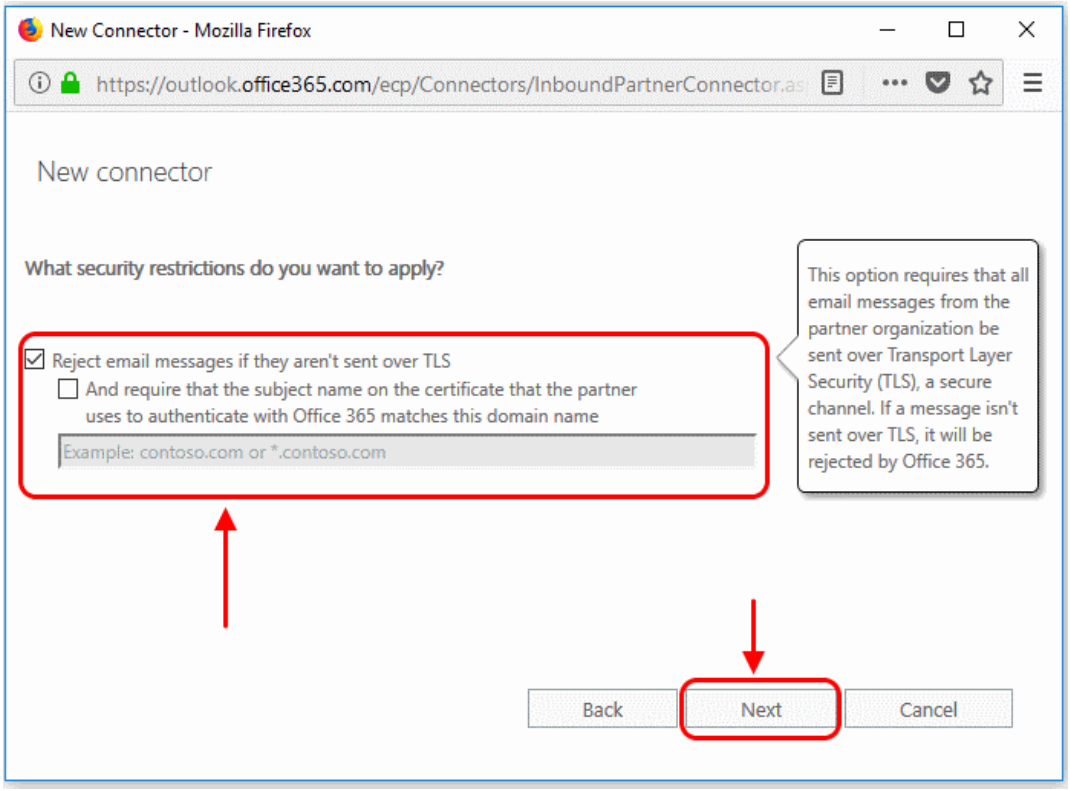


- Enter the IP addresses of the organization you want to add to the safe list. This will be the IP address of your KoruMail Server. This information is provided by Comodo to you by email after the provisioning step is finished.

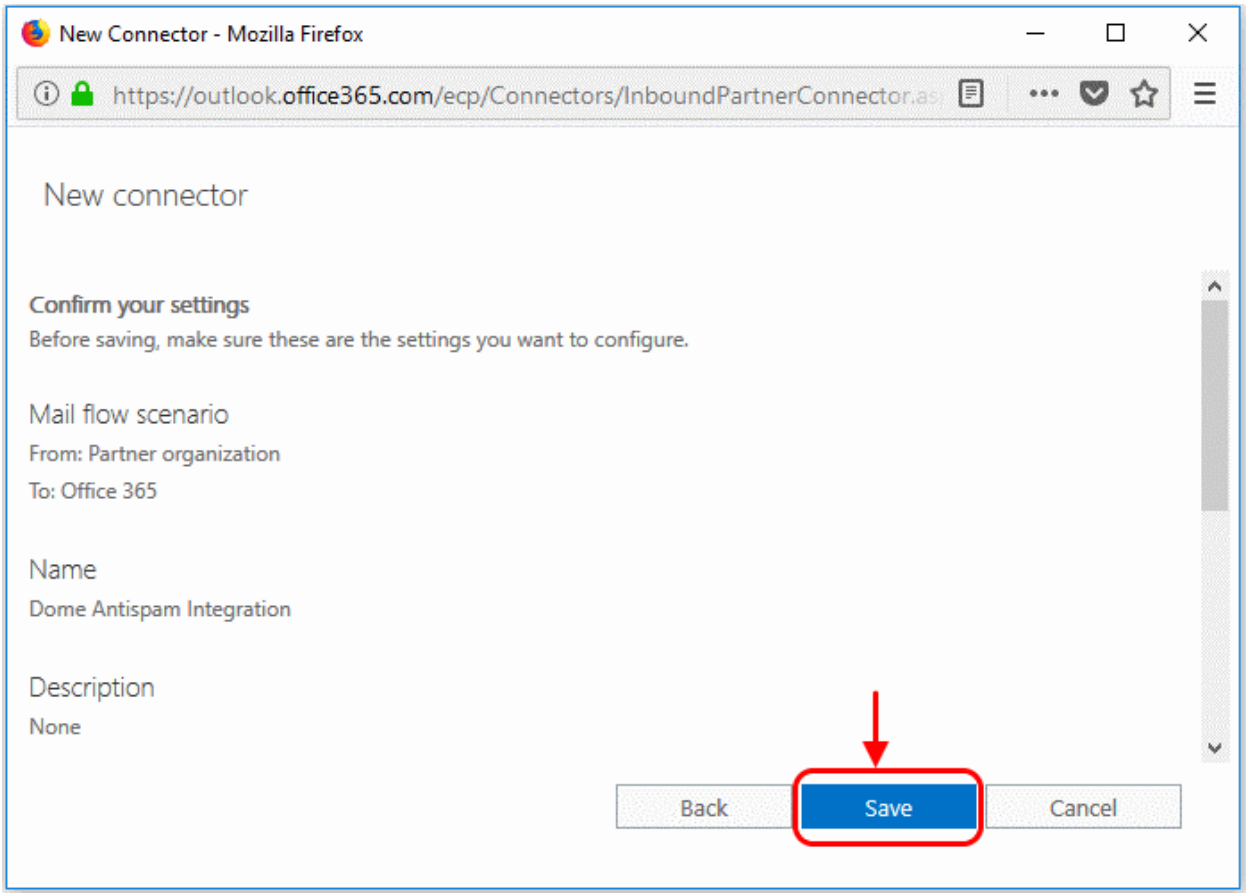
Note: IP ranges should be in the format nnn.nnn.nnn.nnn/rr

Office 365 only accepts ranges (rr) between 24 and 32. Please change the rr from the Korumail instructions to the closest Office 365 allows you to set. For example, if the range you were provided with is 216.104.0.0/19, you can enter 216.104.0.0/24.

- Select the security restrictions you want:



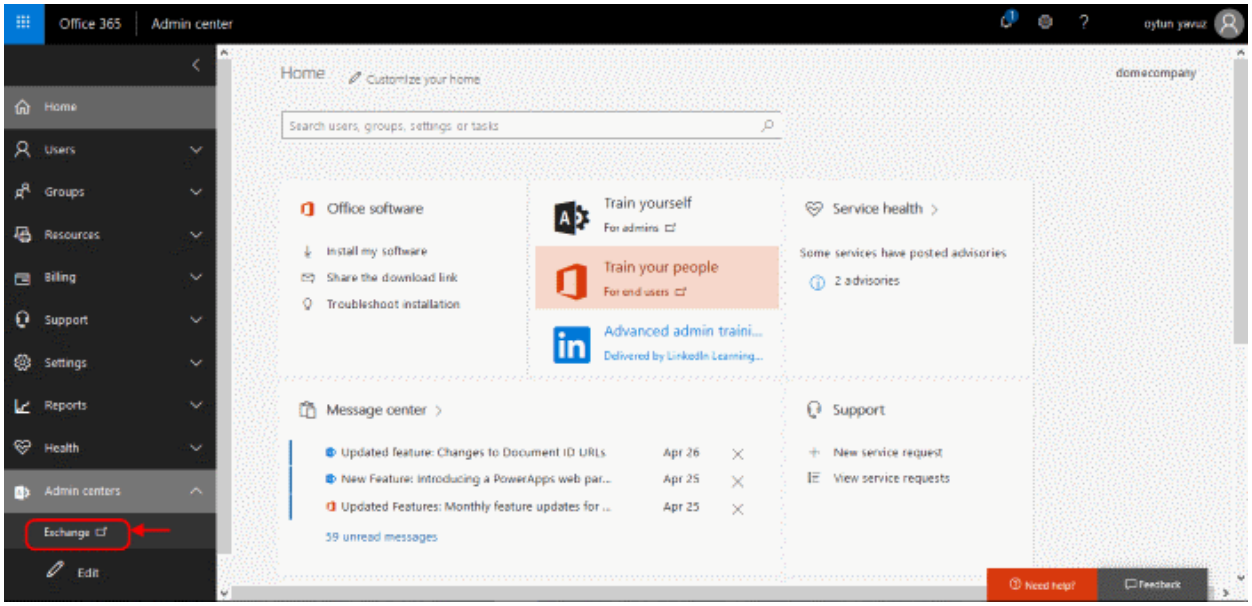
- Click 'Save' to confirm



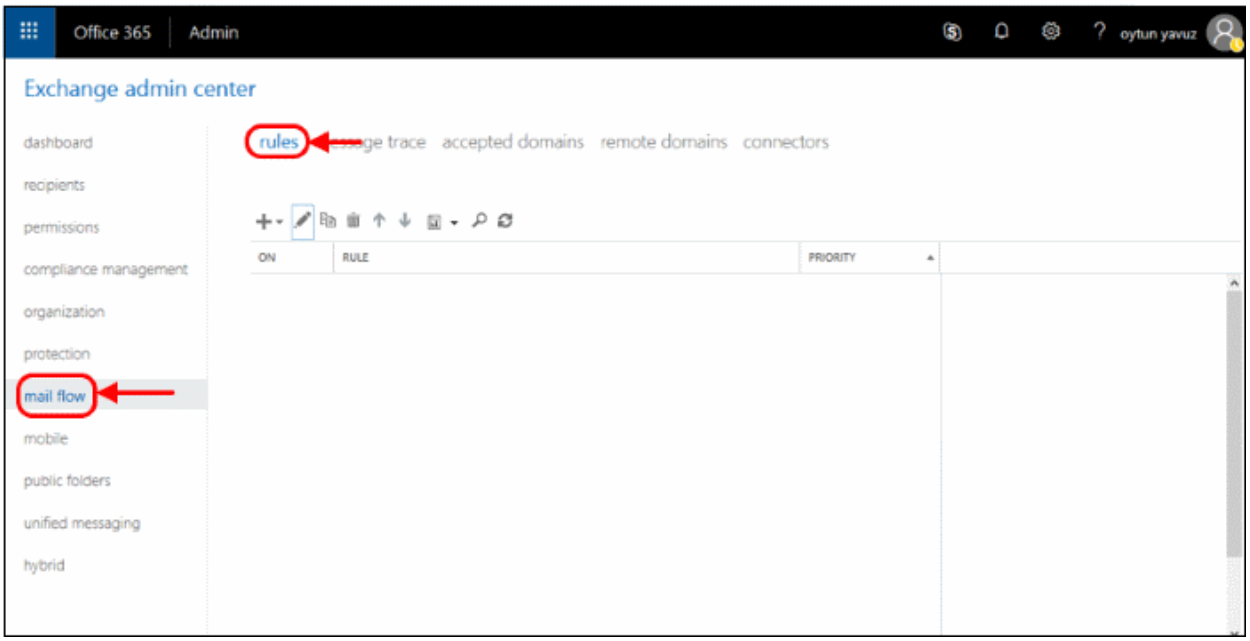
3.1.1 Add an email flow rule to bypass spam filtering

Turn off spam filtering in Exchange Online so you can use Comodo KoruMail instead.

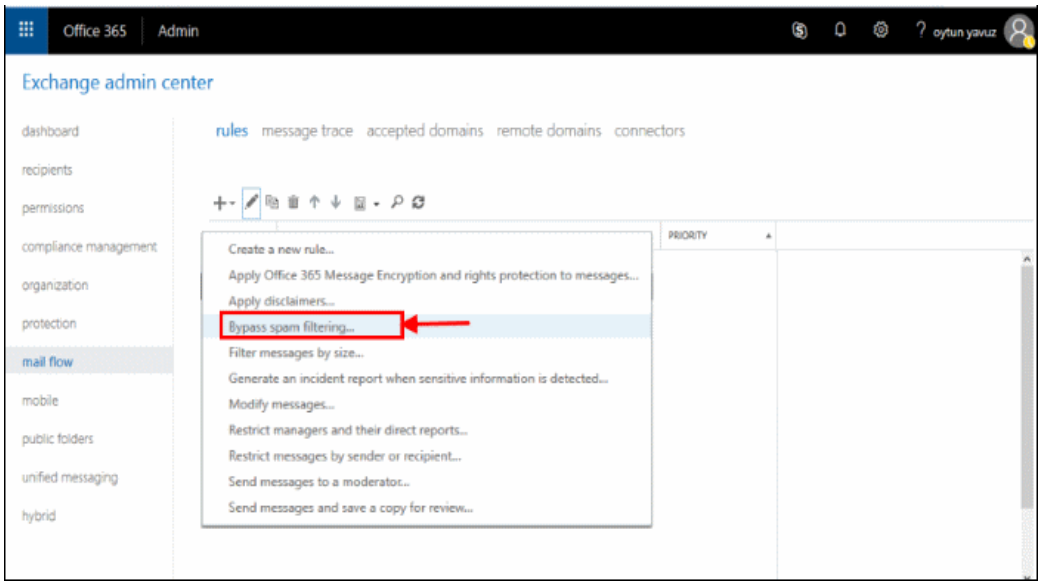
- Log in to your Microsoft Office 365 administrator center account:
  - Click 'Admin' in the left menu
  - Click 'Admin Centers' > 'Exchange':



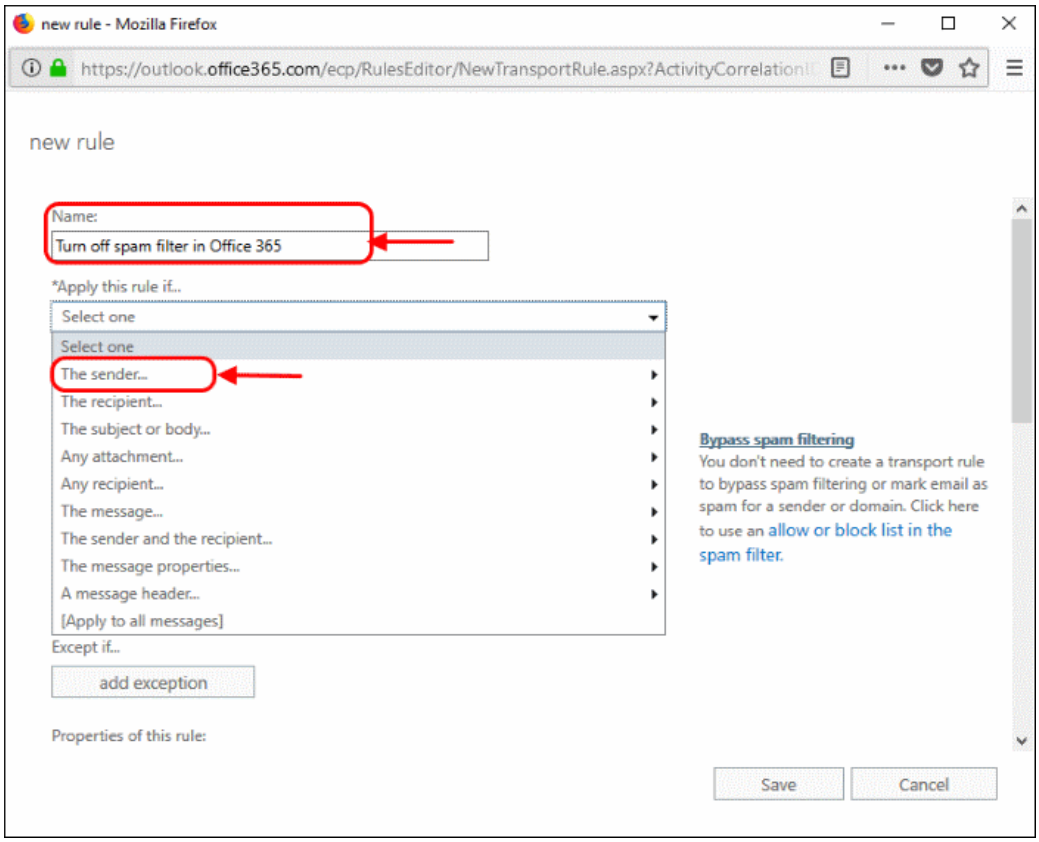
  - Click 'Mail Flow' on the left
  - Click 'Rules' at the top:



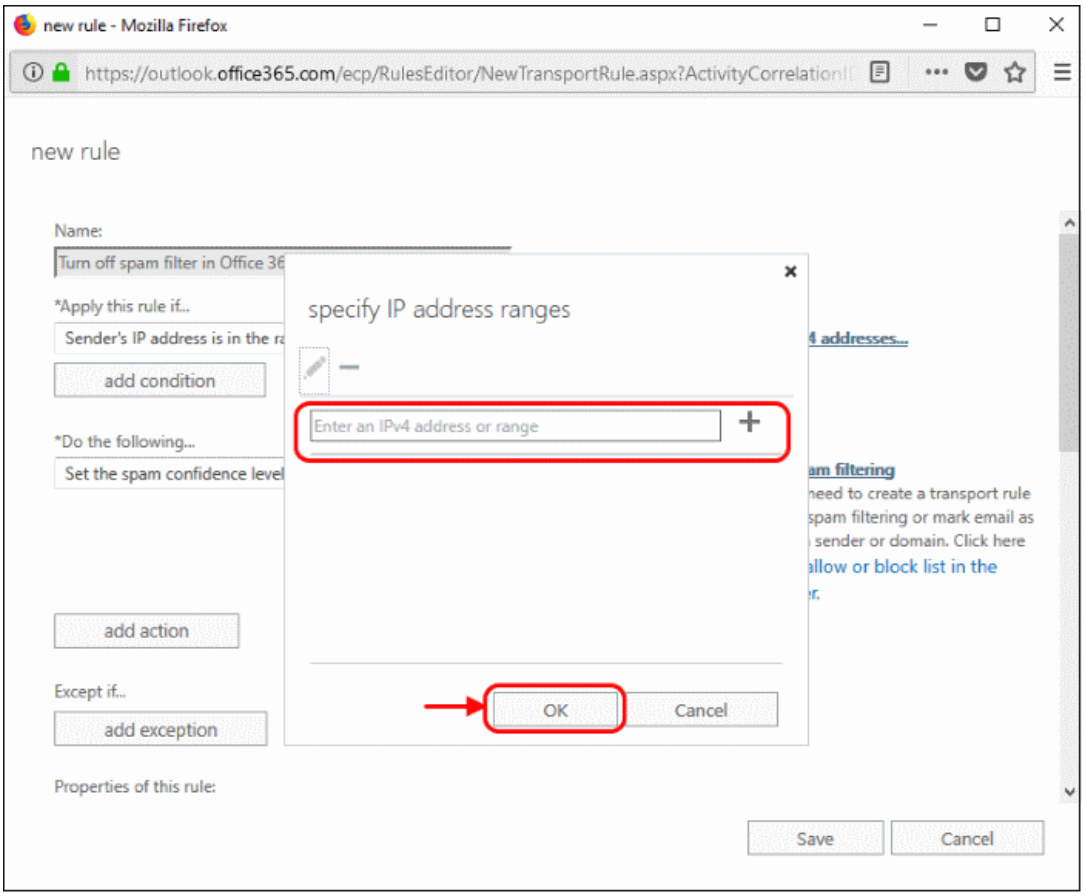
- Select 'Bypass spam Filtering' from the drop-down menu:



- In the 'Rule' window, complete the required fields.
  - Select 'Turn off spam filter in Office 365' in the 'Name' drop-down menu
  - Select 'The Sender' in the 'Apply this rule if..' drop-down menu
    - Select 'The Sender...'

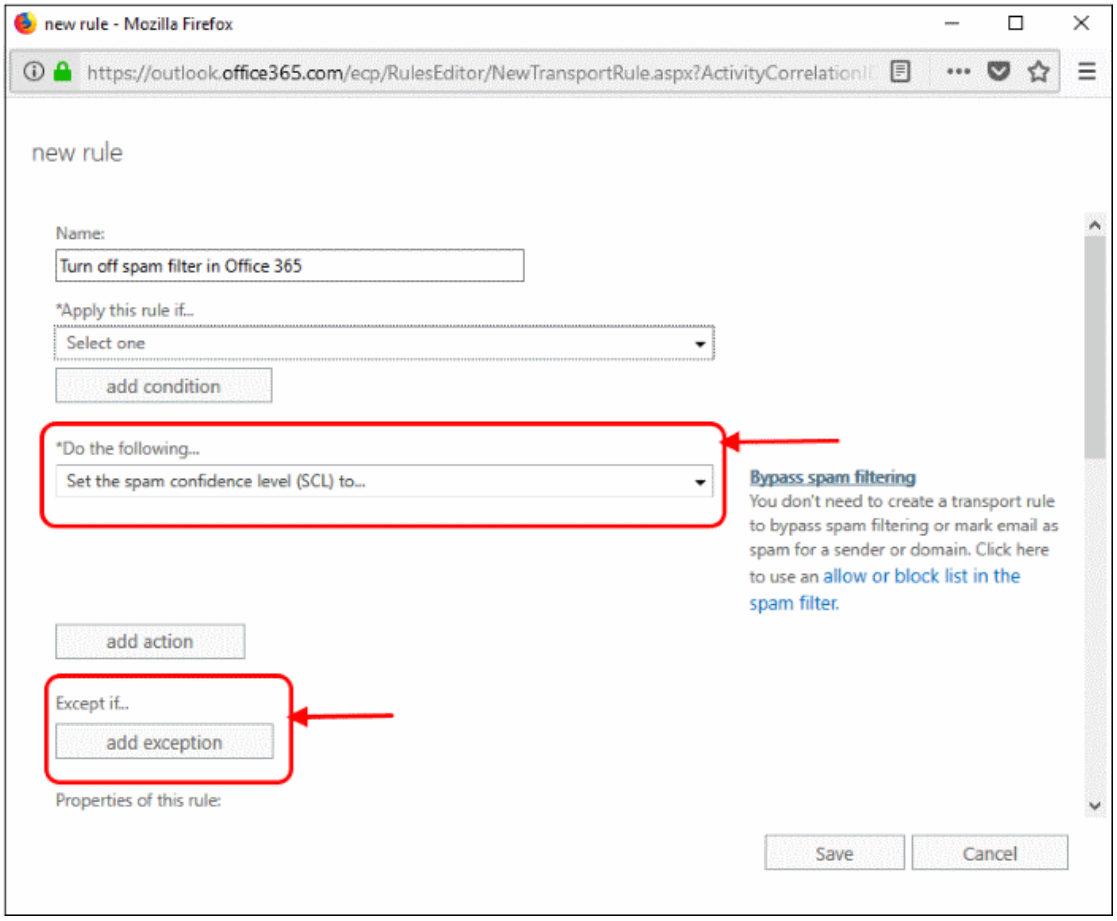


    - Select 'IP Address is in any of these ranges or exactly matches'
    - 'Specify IP address ranges' - enter the same IP addresses from the Inbound Mail flow setup section above



- Click '+' for each range
- Click 'OK'

- 'Do the following' - Set the spam confidence level (SCL) to 'Bypass spam filtering'
- 'Except if' - Do not add an exception



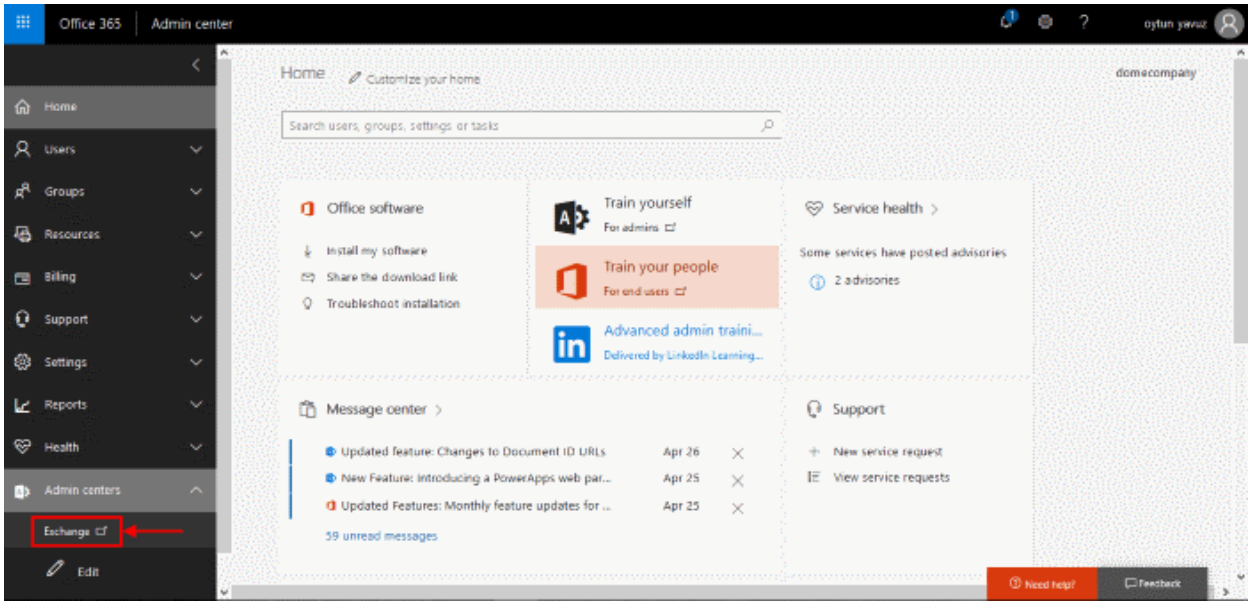
- Deselect the 'Audit this rule with severity level' option
- Select 'Enforce' from 'Select the mode for this rule'

- Click 'Save'

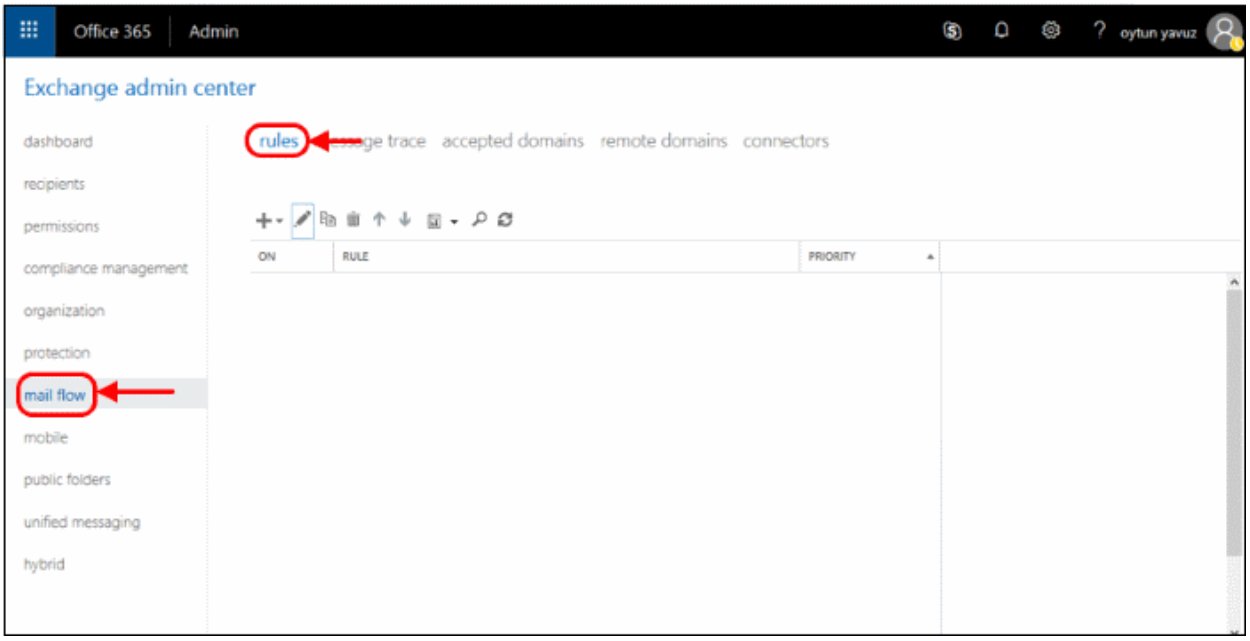
3.1.2 Add an email flow rule to lock down Exchange Online

This rule ensures Exchange will only accept mails from Korumail. This stops spammers bypassing Korumail and flooding your network with junk mail.

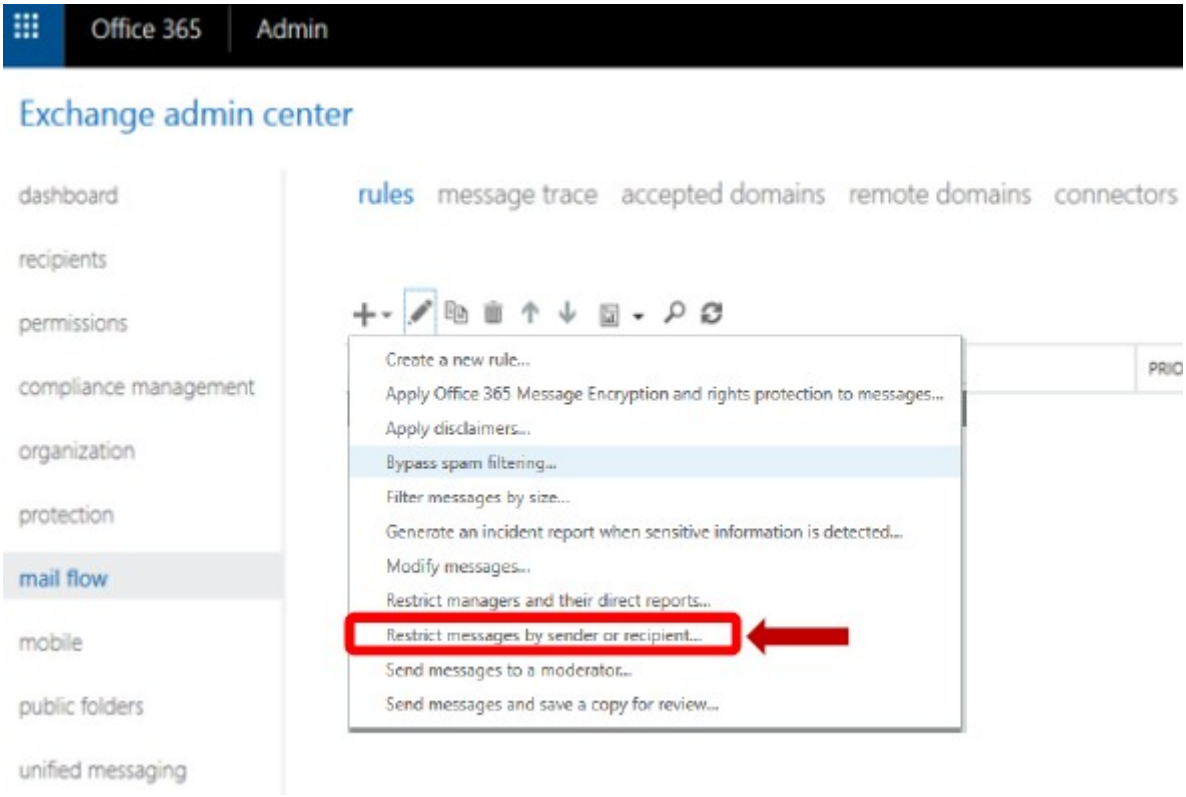
- Log into your Microsoft Office 365 administrator center account
  - Click 'Admin' in the left-hand menu
  - Click 'Exchange':



  - Click 'mail flow' on the left
  - Click 'rules' in the top navigation:

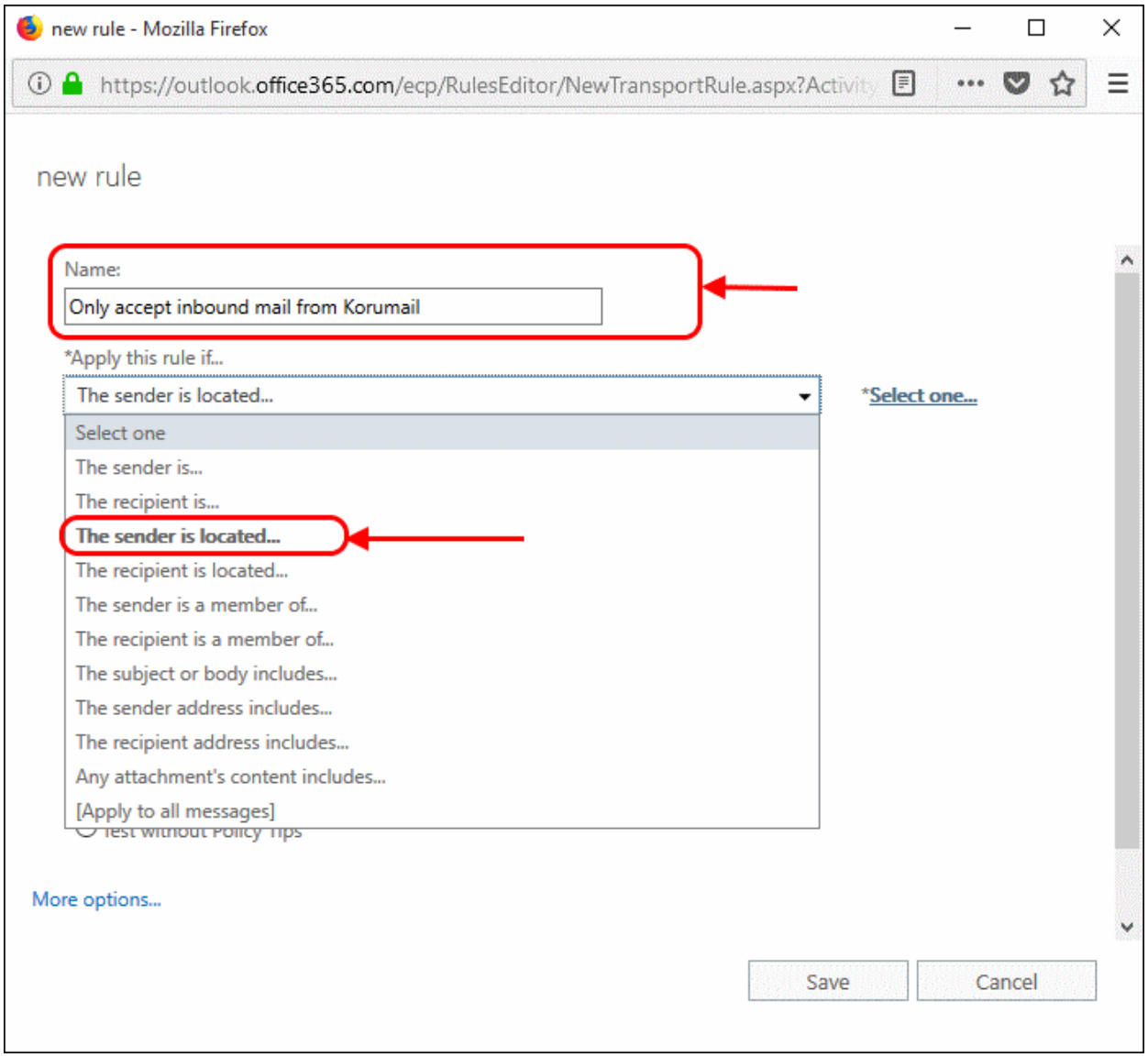


  - Click the pencil icon
  - Select 'Restrict messages by sender or recipient'

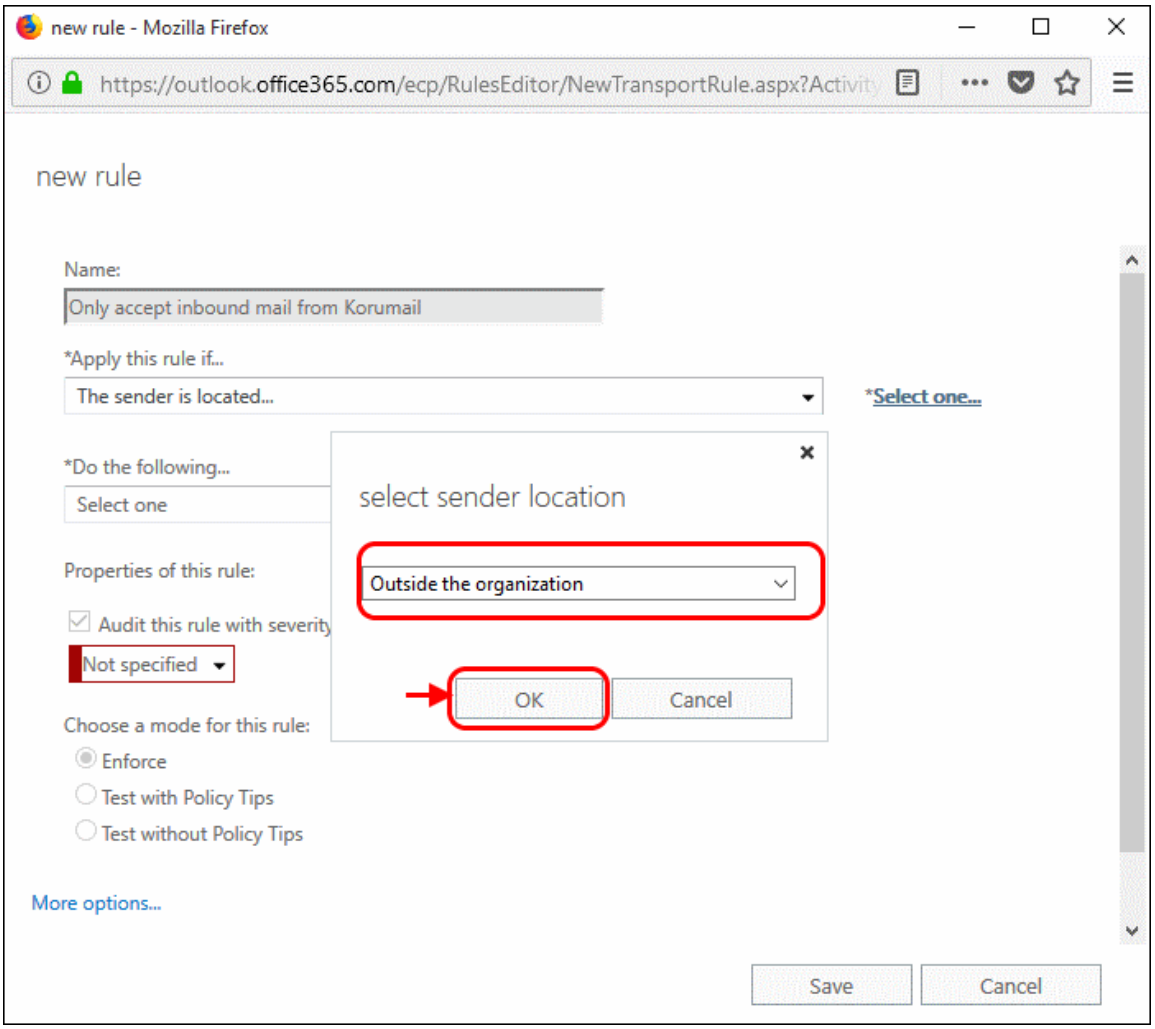


In the create rule screen:

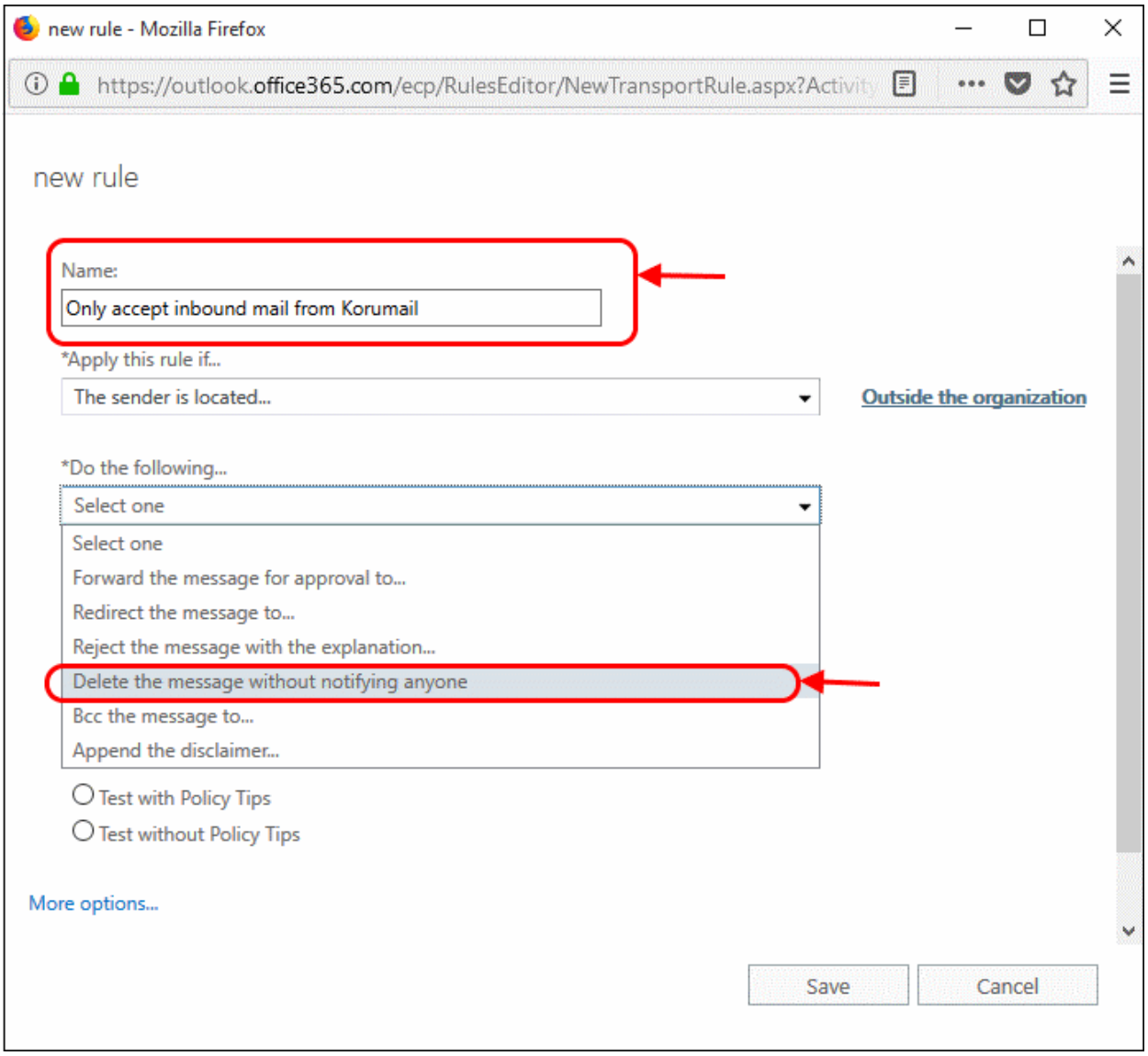
- **Name**: Call the rule 'Only accept inbound mail from Korumail'
- **Apply this rule if**: Choose 'The Sender is located...' :



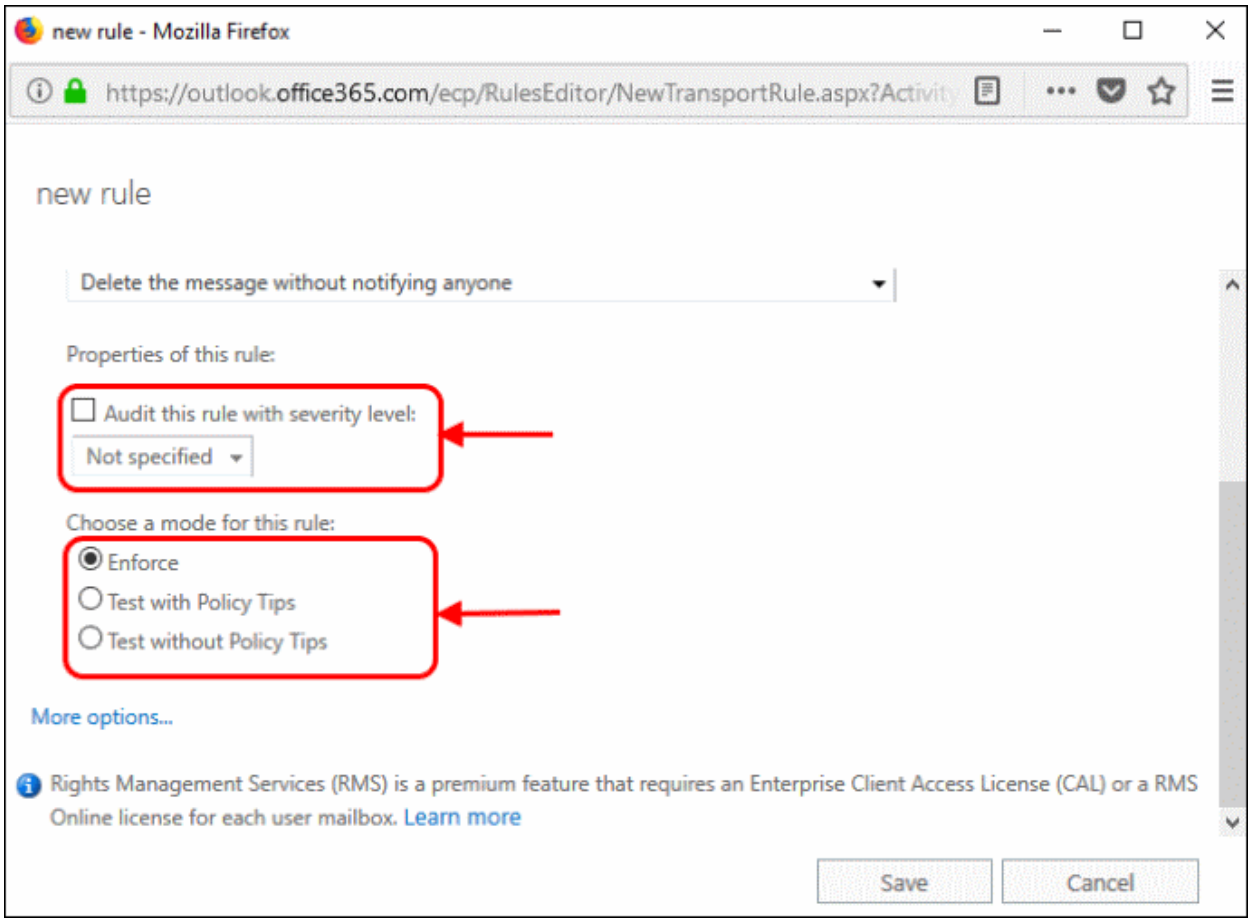
- This will open a pop-menu. Select 'Outside the organization' from the menu
- Click 'OK':



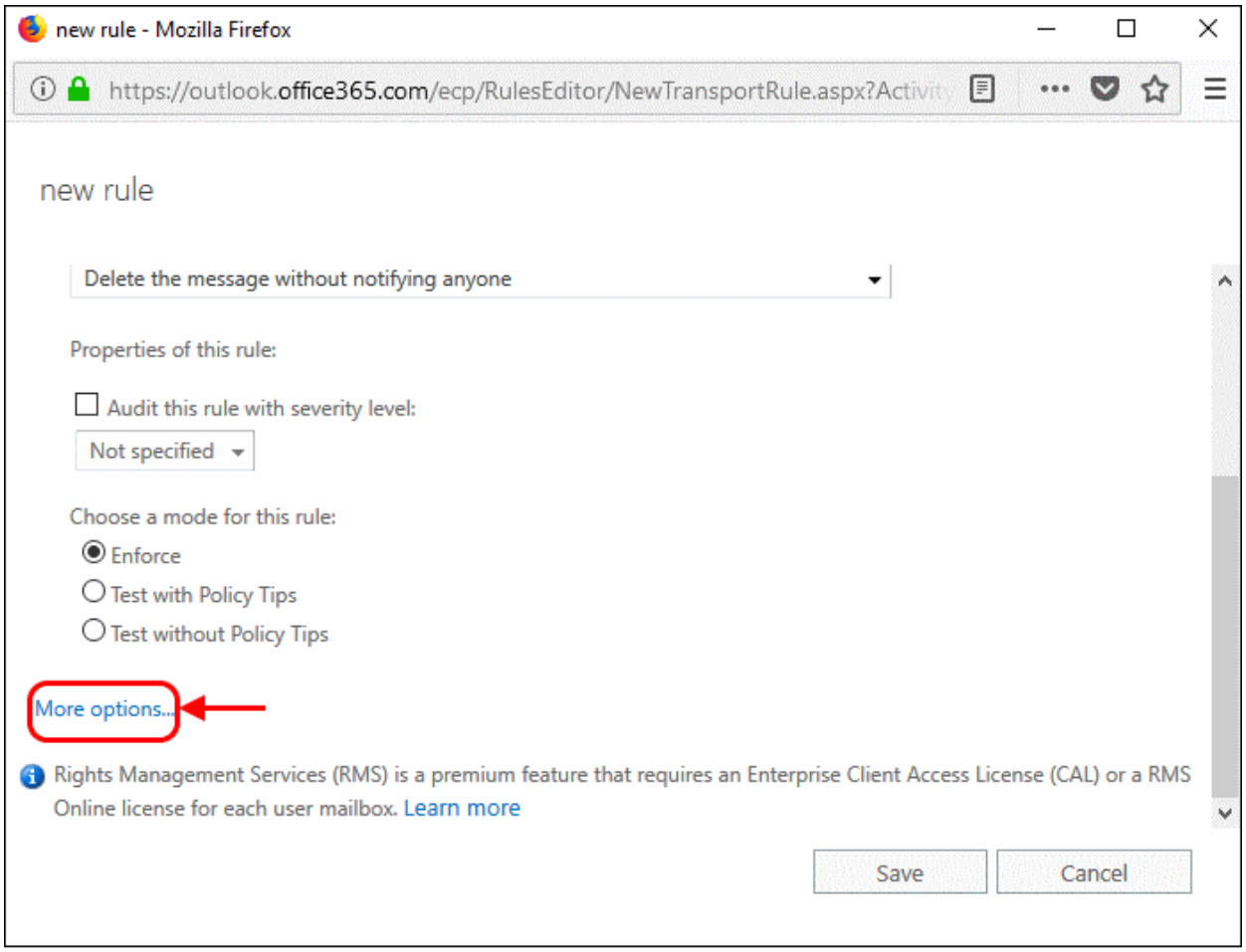
- **Do the following**: Select 'Delete the message without notifying anyone':



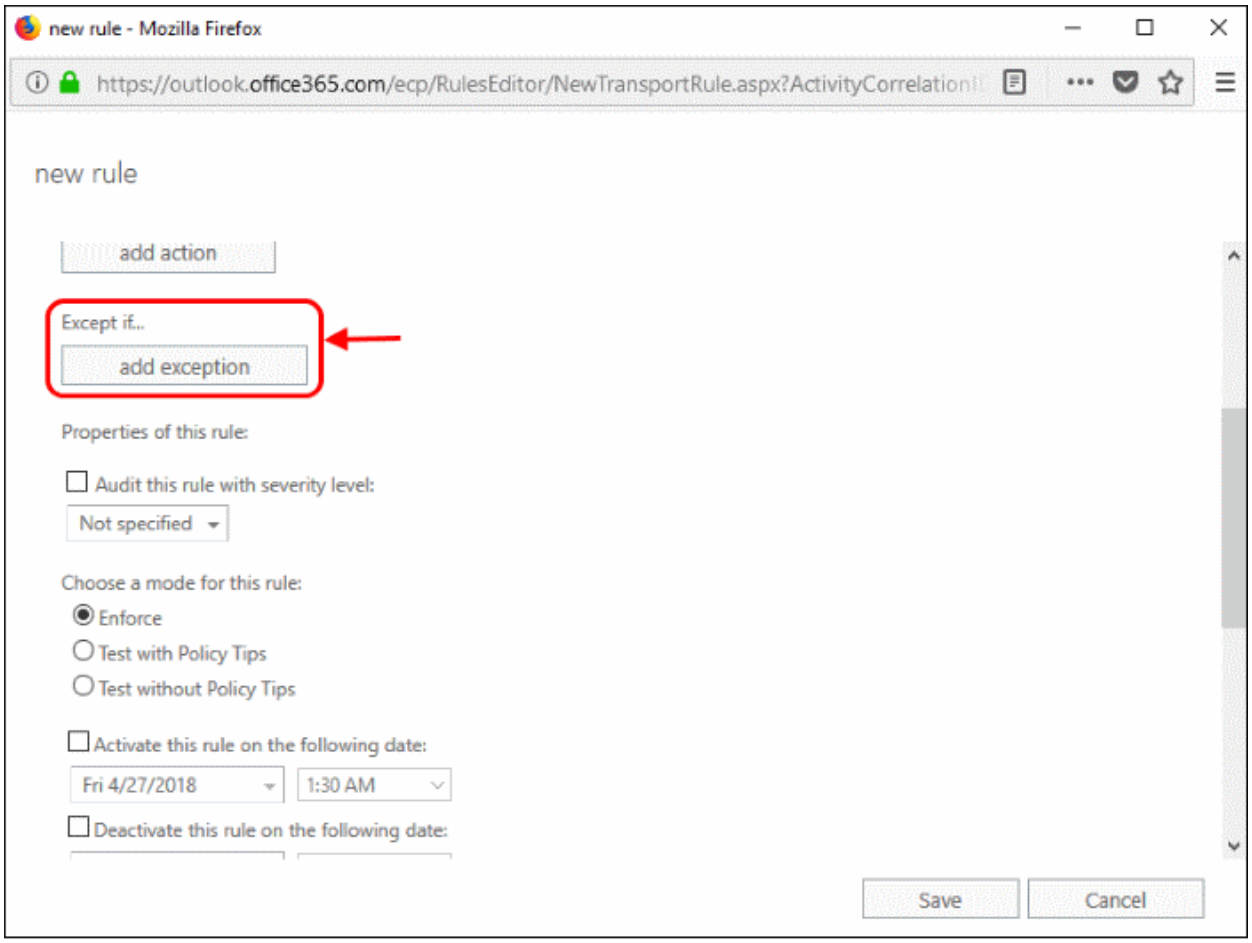
- **Audit this rule with severity level** - Deselect this option
- **Choose a mode for the rule** - Select 'Enforce'



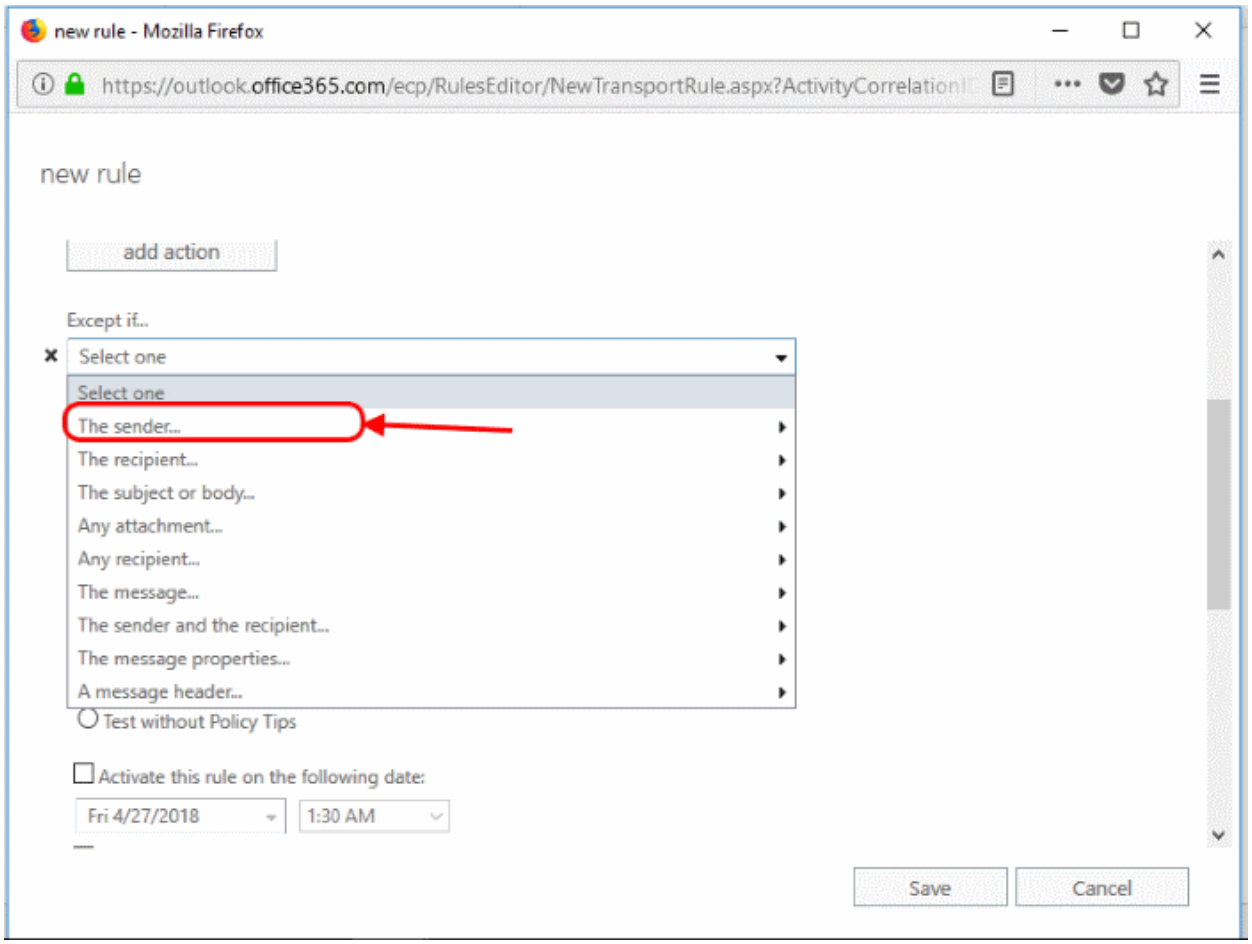
- Next, we add an exception to allow email from Korumail
  - Click 'More Options'



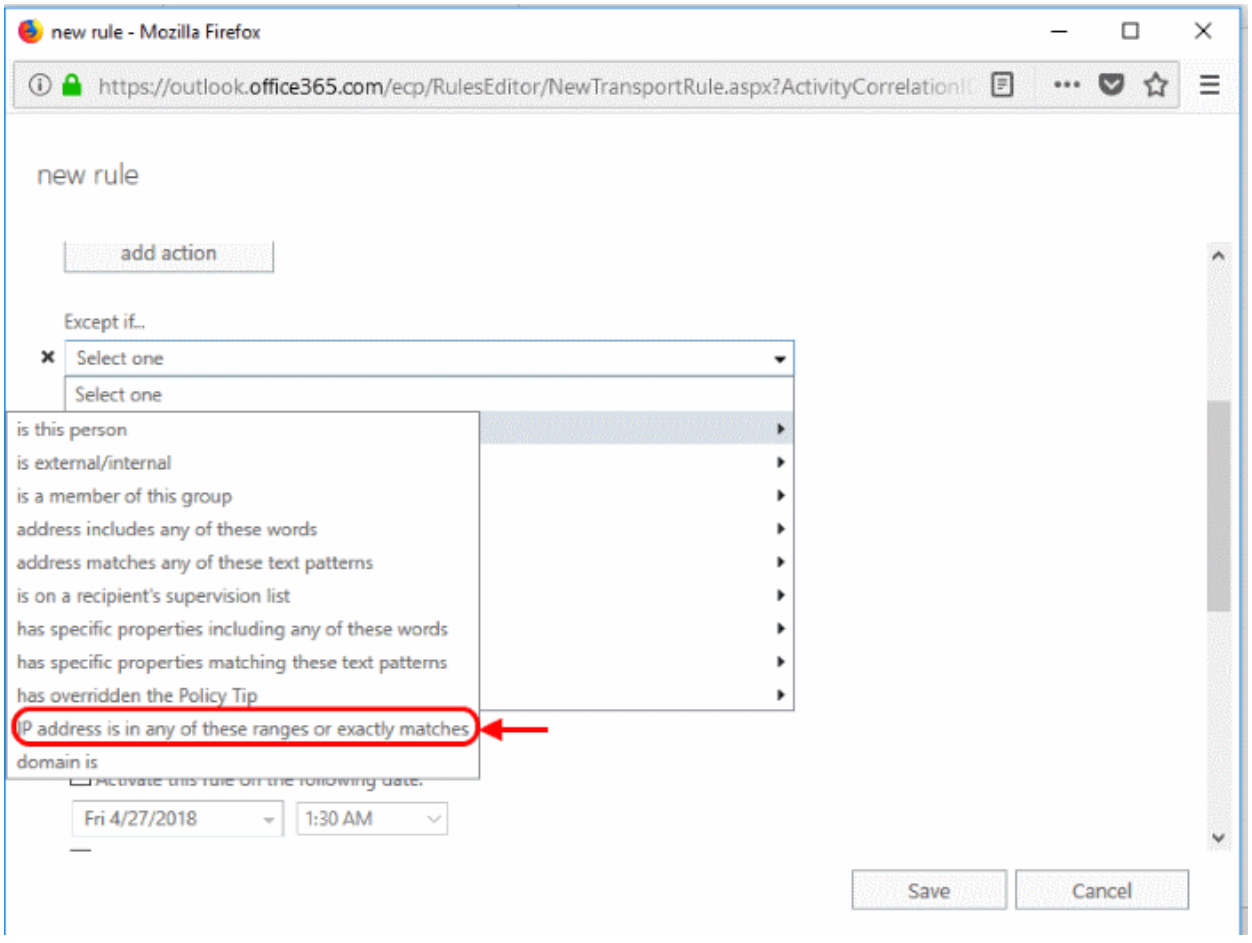
- 'Except if' – click the 'Add Exception' button:



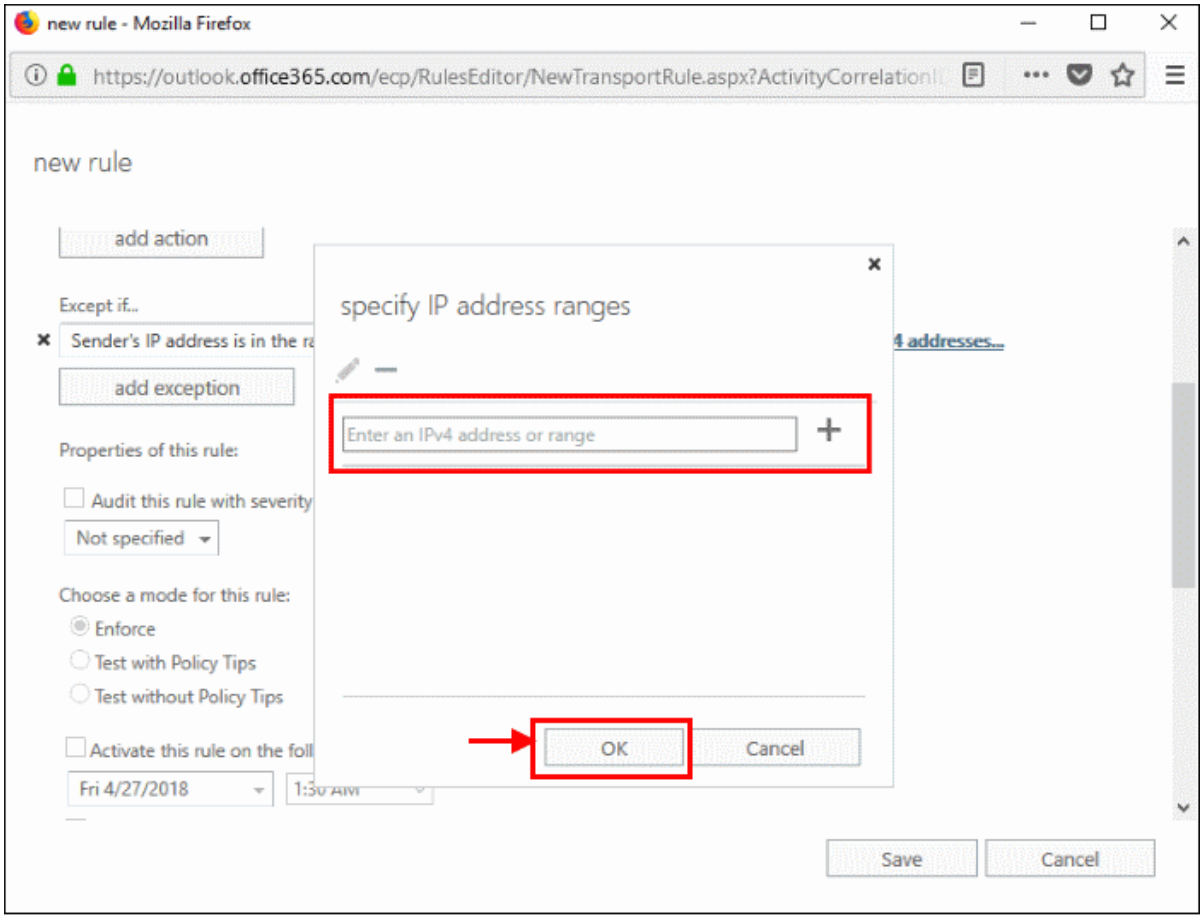
- Select 'The Sender':



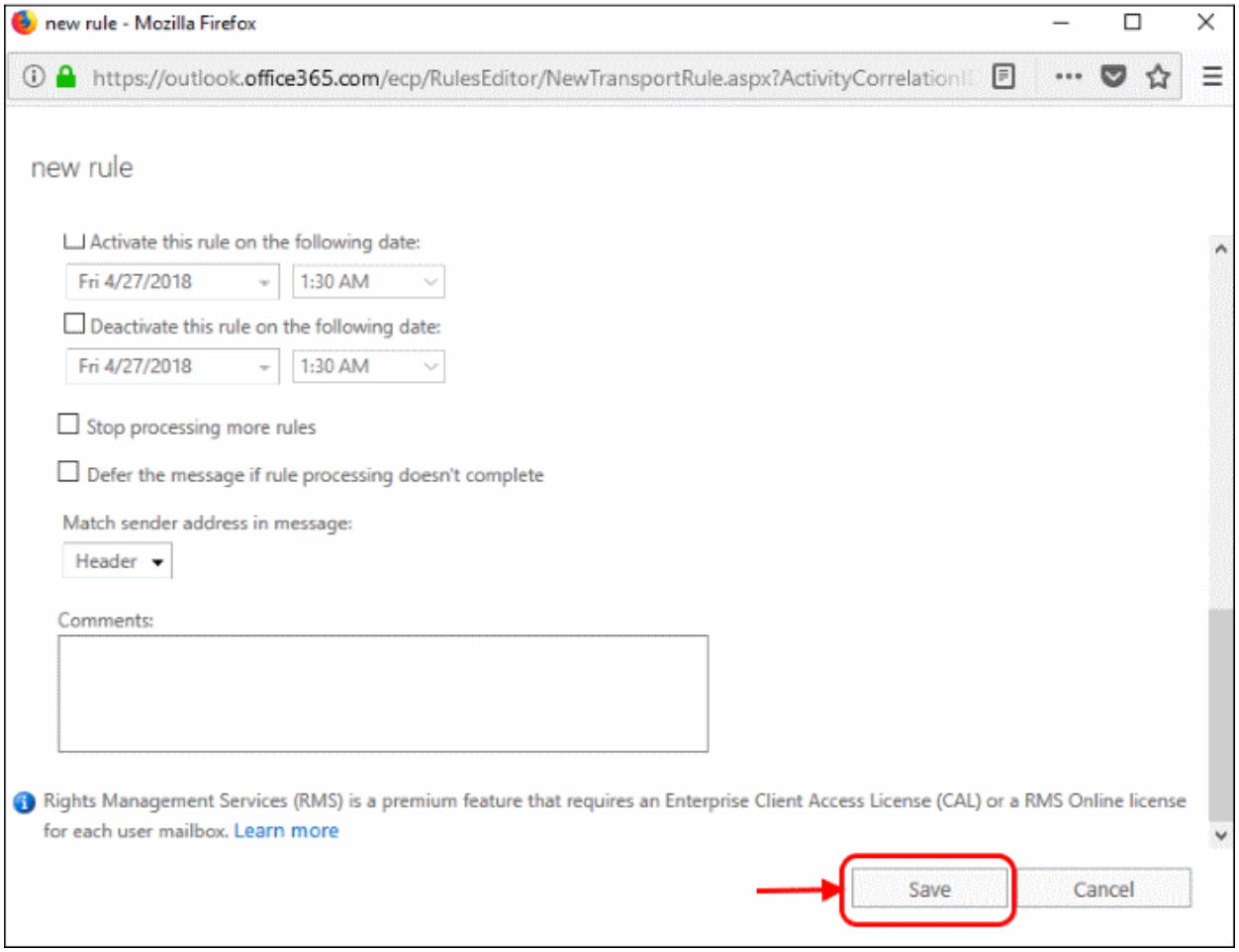
- Select 'IP address is in any of these ranges or exactly matches':



- Specify IP address ranges window - select the IP addresses you added in the **Inbound Mail Flow Setup** section:



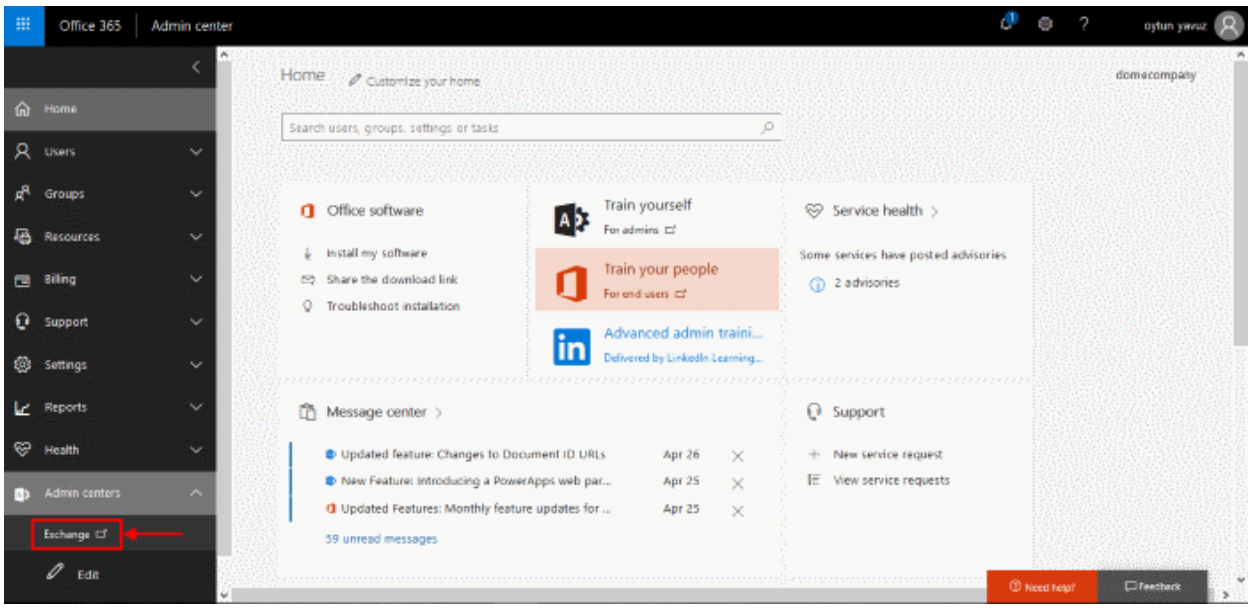
  - Click '+' icon for each range
  - Click 'OK'
- Click 'Save'



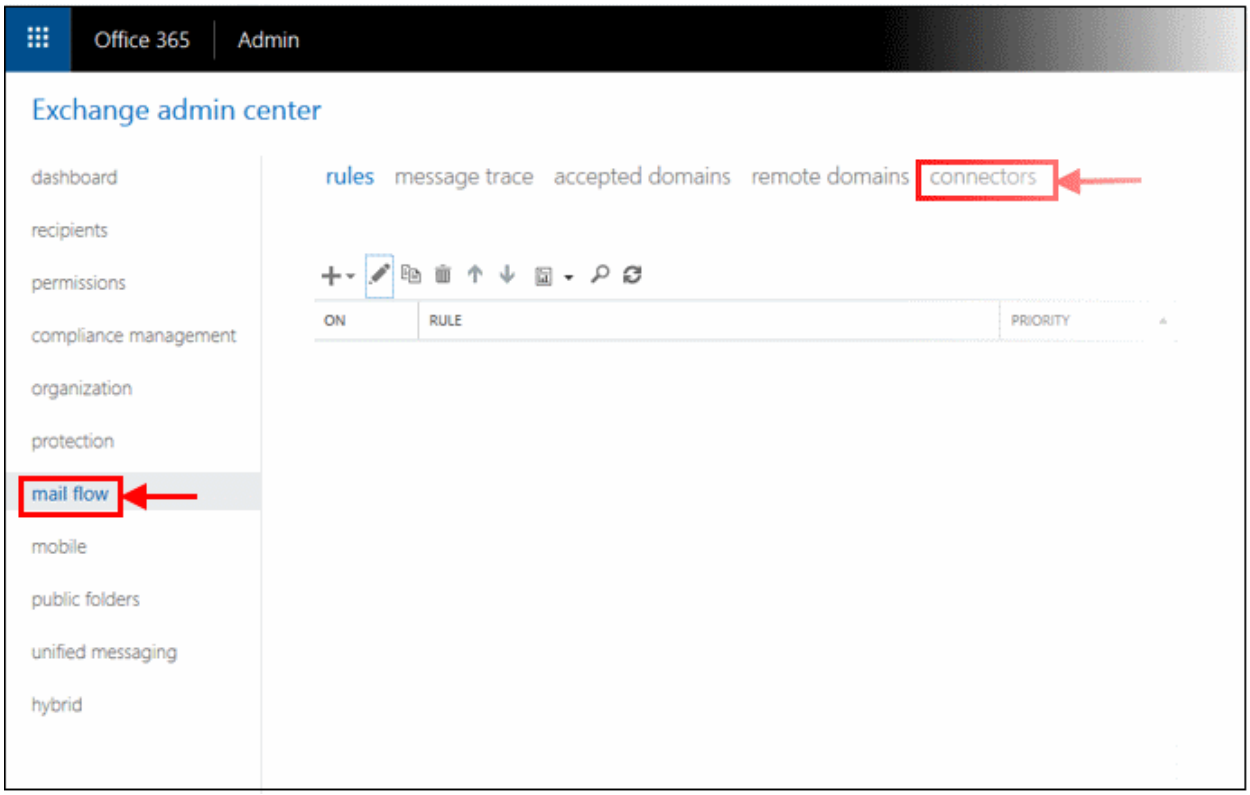
3.2 Outbound flow setup on Office 365

To set up outbound flow set up in Office 365:

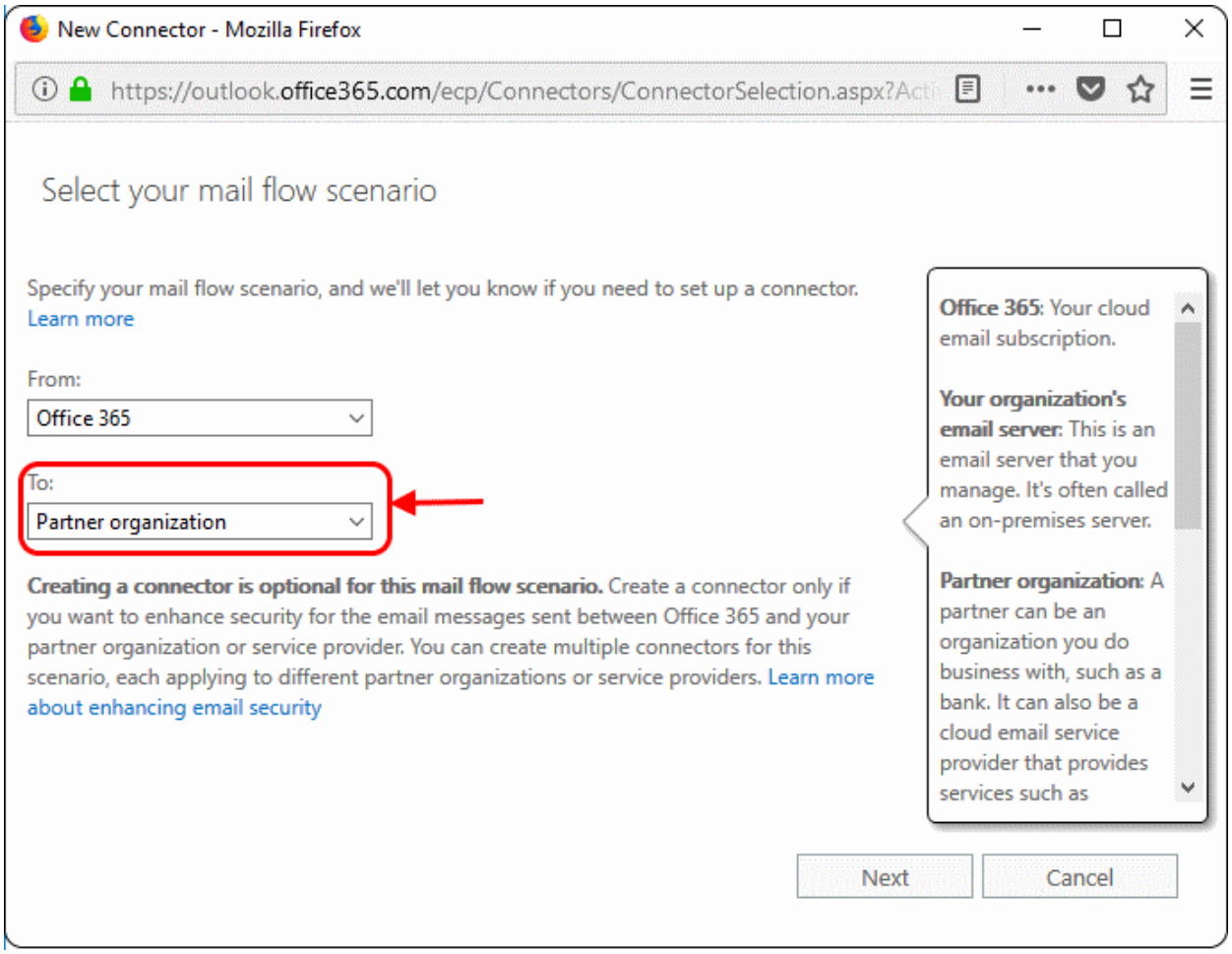
- Login to your Microsoft Office 365 administrator center account
  - Click 'Admin' in the left-hand menu
  - Click 'Exchange':



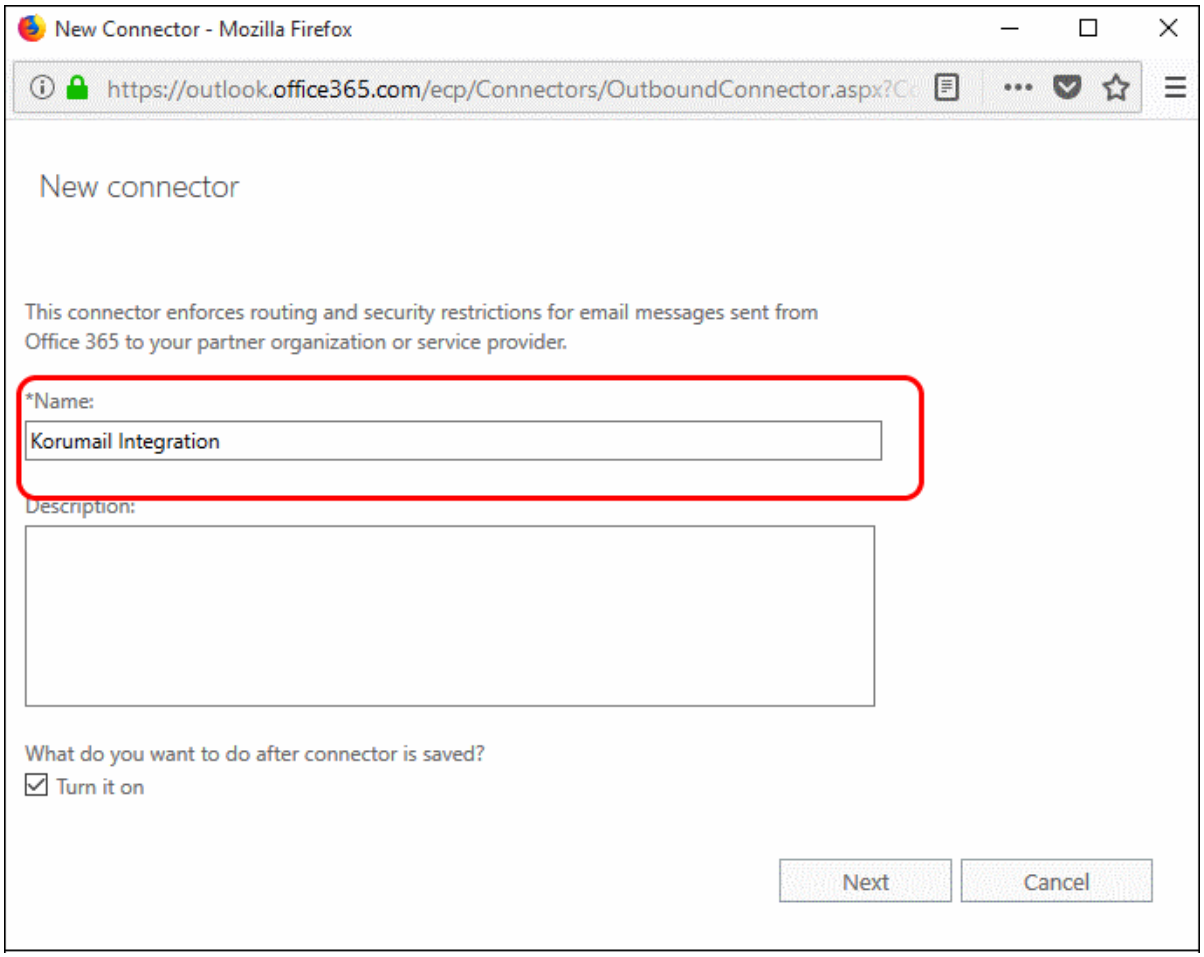
- Click 'mail flow' on the left
- Click 'connectors' in the top navigation:



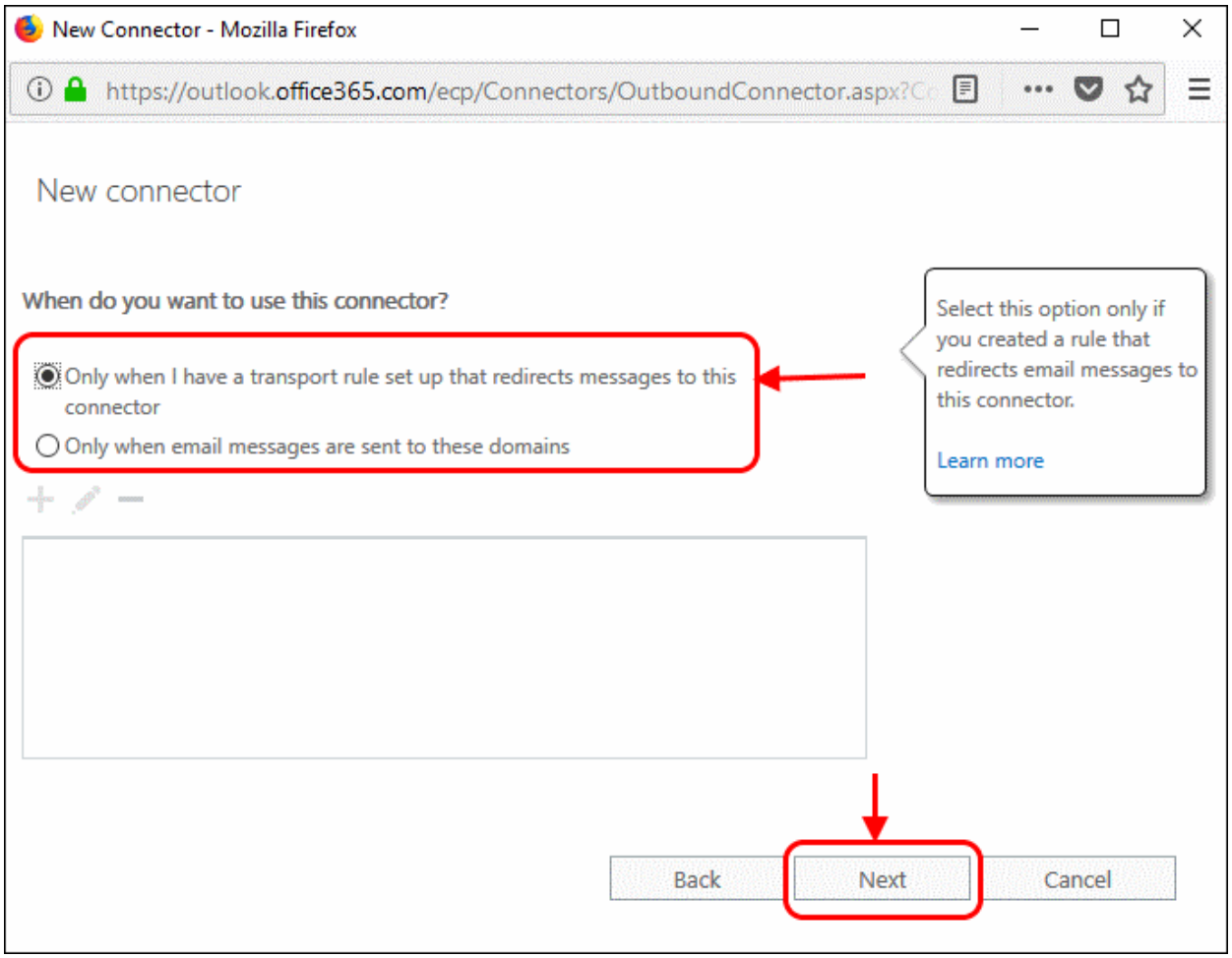
- To add an 'Outbound Connector':
  - Select 'Office 365' in the 'From' drop-down menu
  - Select 'Partner Organization' in the 'To' drop-down menu:



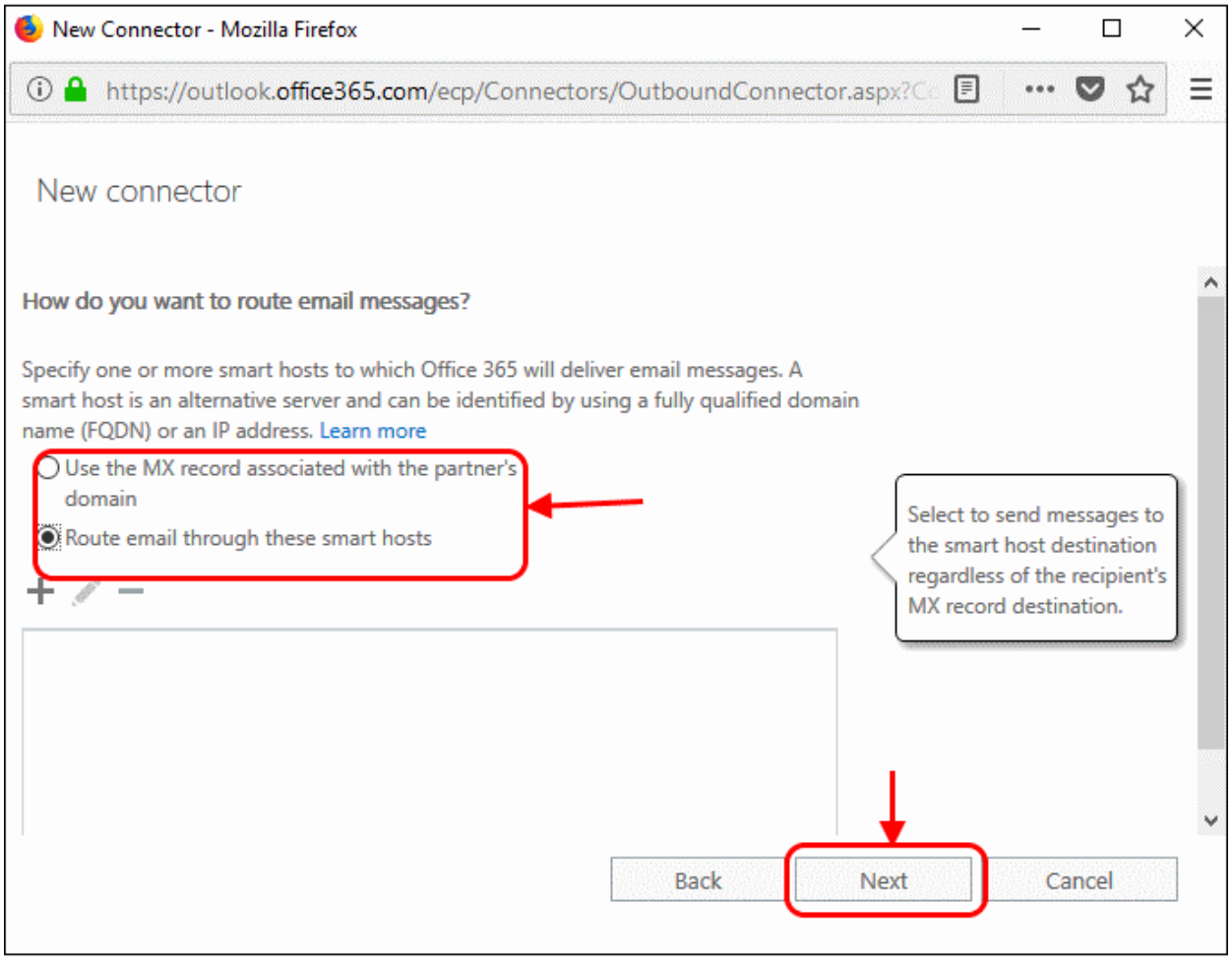
- Click 'Next'.
- Enter a descriptive name for the outbound connector in the 'Name' field
- Click 'Next'



- '**When do you want to use this connector?**' - Select 'Only when I have a transport rule set up that redirects messages to this connector'
- Click 'Next':



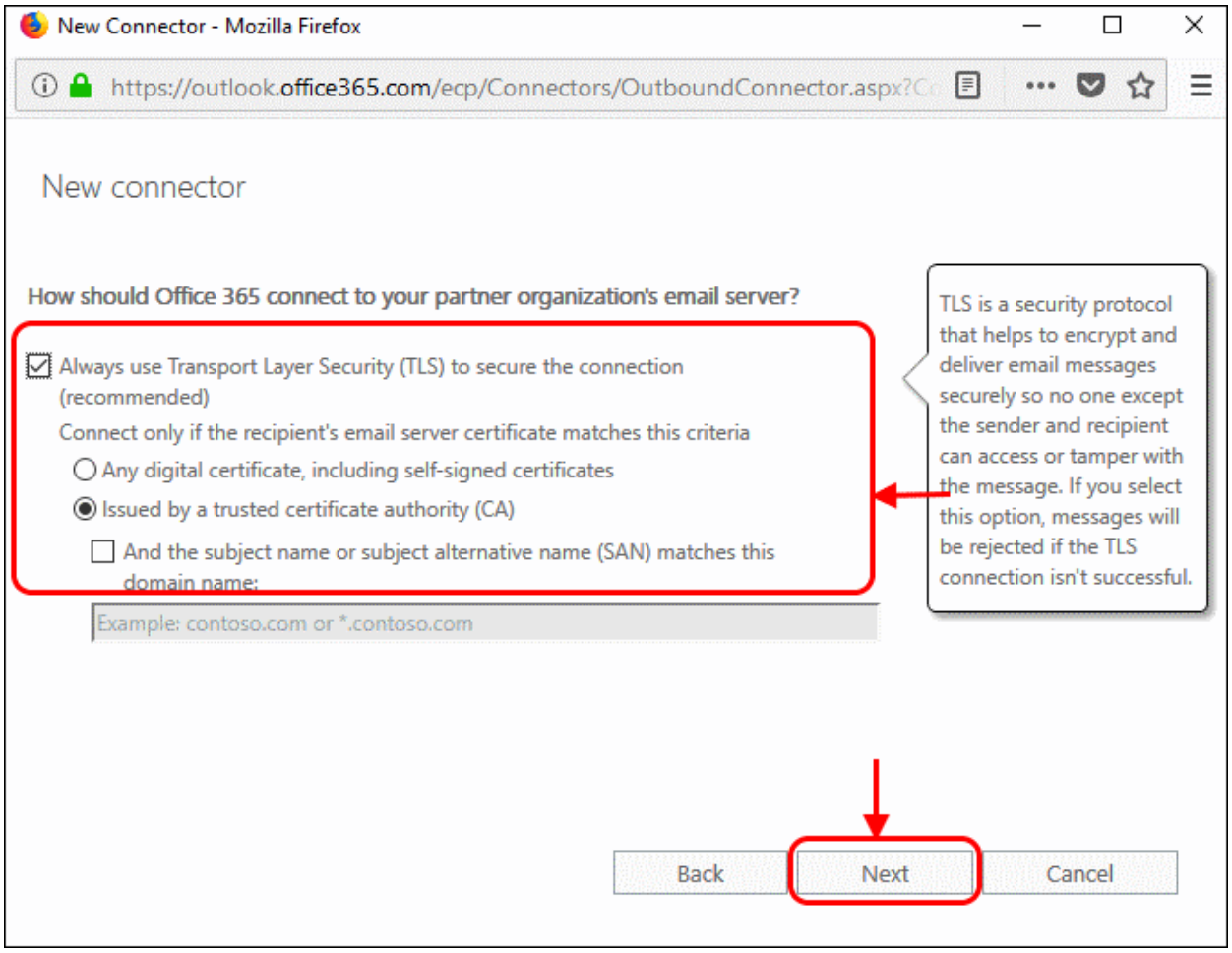
- 'How do you want to route email messages'
  - Select 'Route through these smart hosts'
  - This will relay messages to the Korumail MTA.
  - The FQDN is in the confirmation email sent to you after we finished provisioning your Korumail instance.
- Enter the FQDN in the space provided then click 'Next':



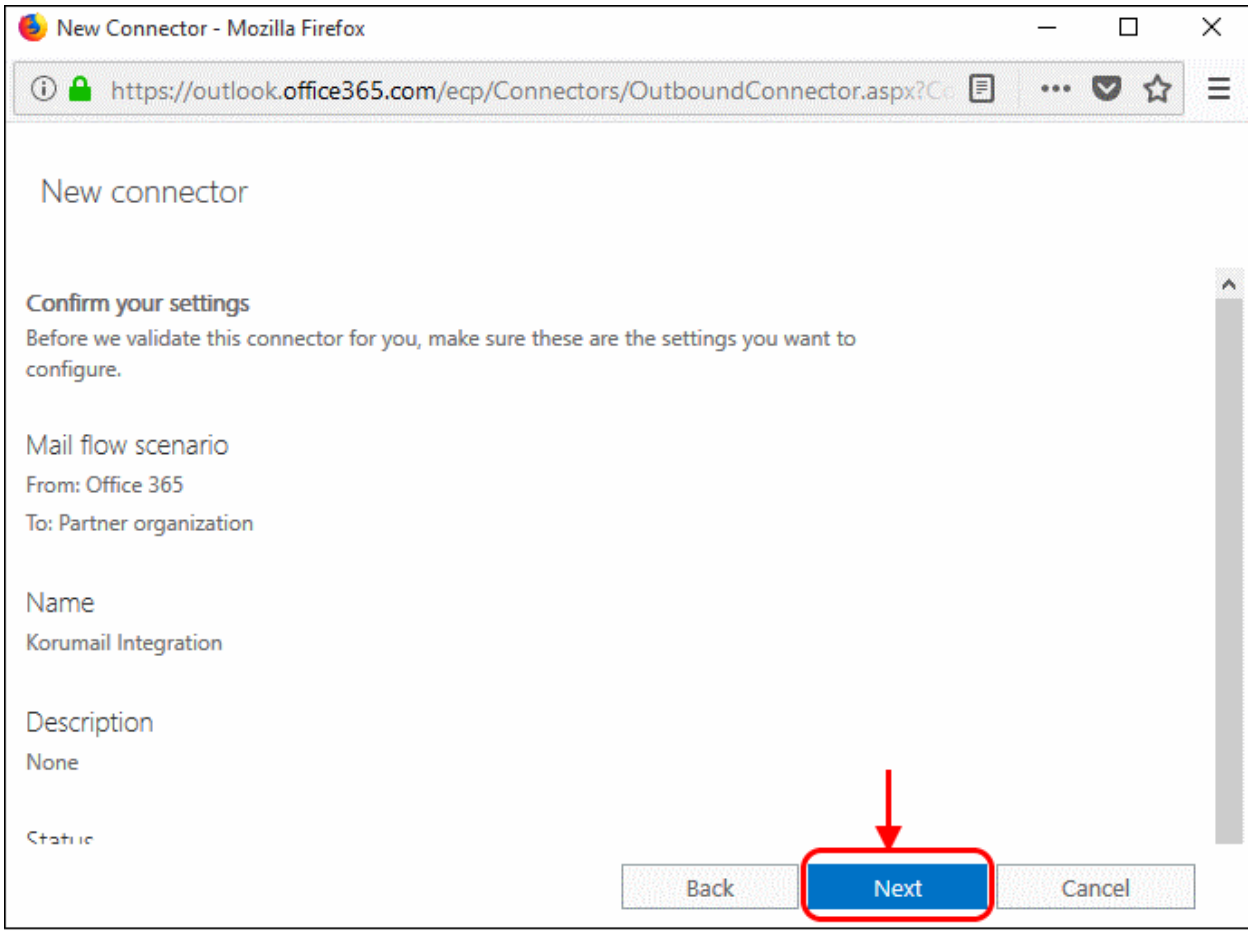
- '**How should Office 365 connect to your partner organization's email server?**' - Select:
  - 'Always use Transport Layer Security (TLS) to secure the connection'

    AND
  - 'Issued by a trusted certificate authority'.

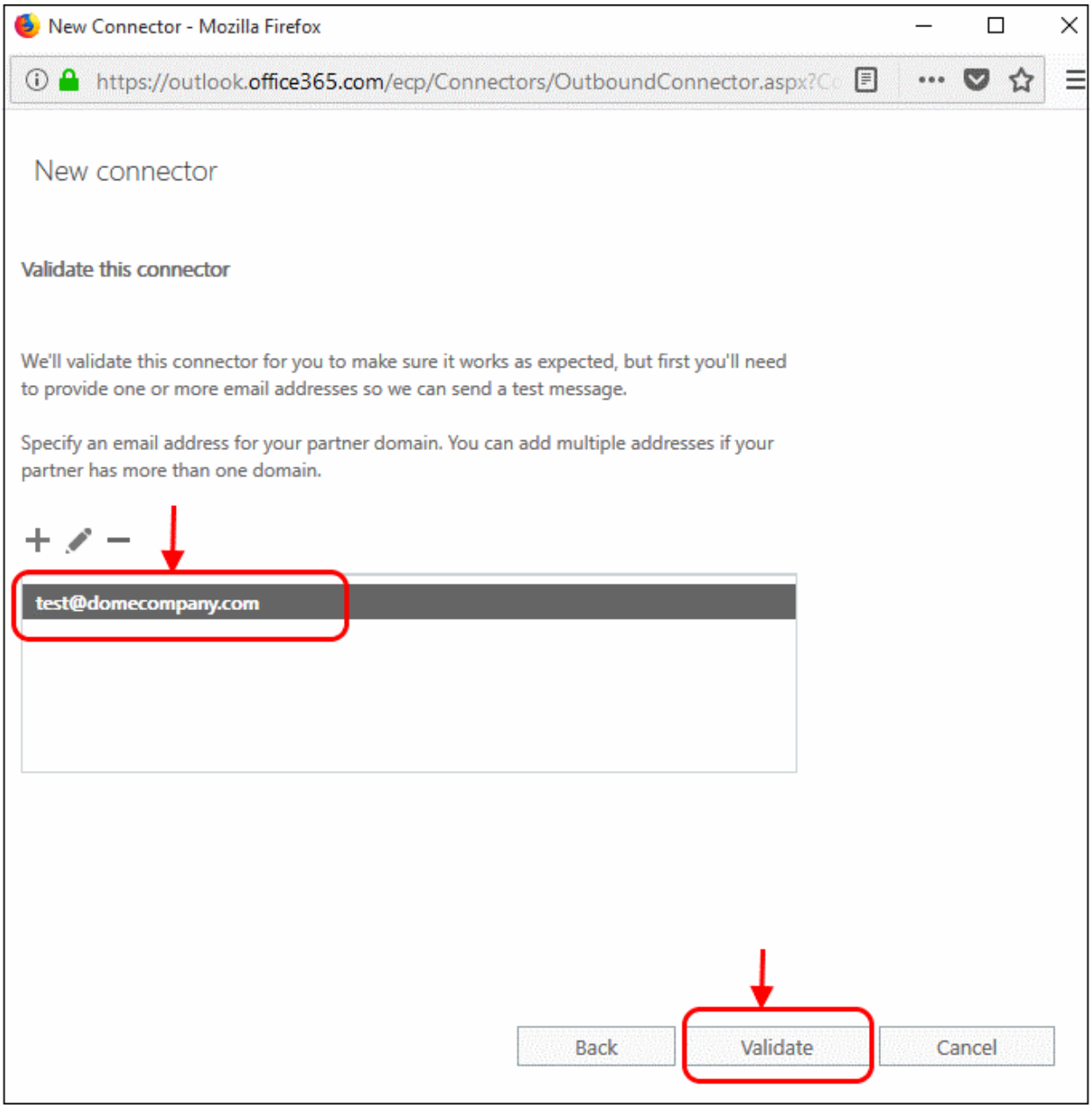
    This will make sure the connection to the mail server is securely encrypted and authentic.
- Click 'Next'



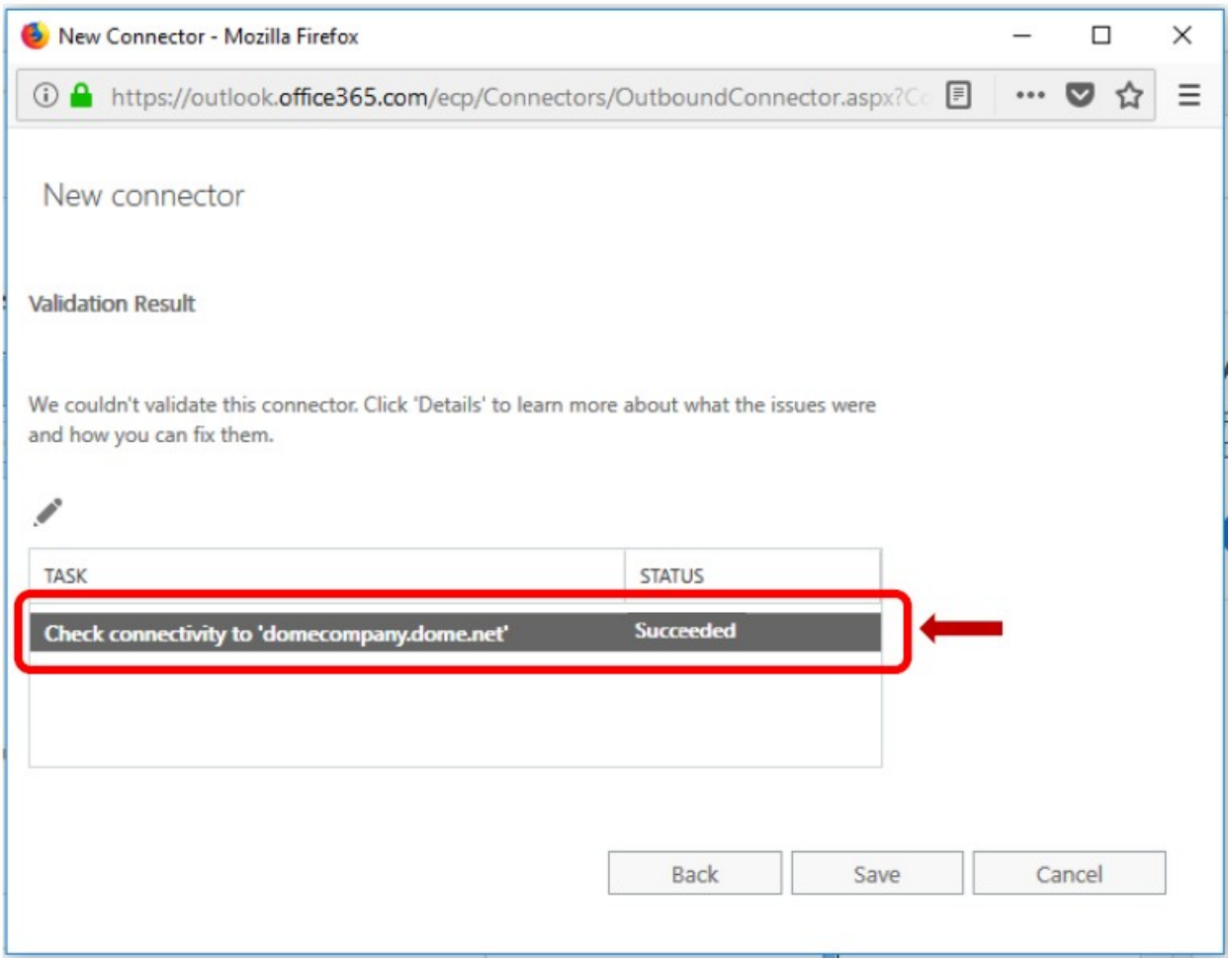
- Review your settings. Check all information in the confirmation screen is as it should be, then click 'Next':



- '**Validate this connector**' - Add an email address at which you can receive mail in the field provided, then click 'Validate'. Office 365 will send you an email to test all settings are correct:



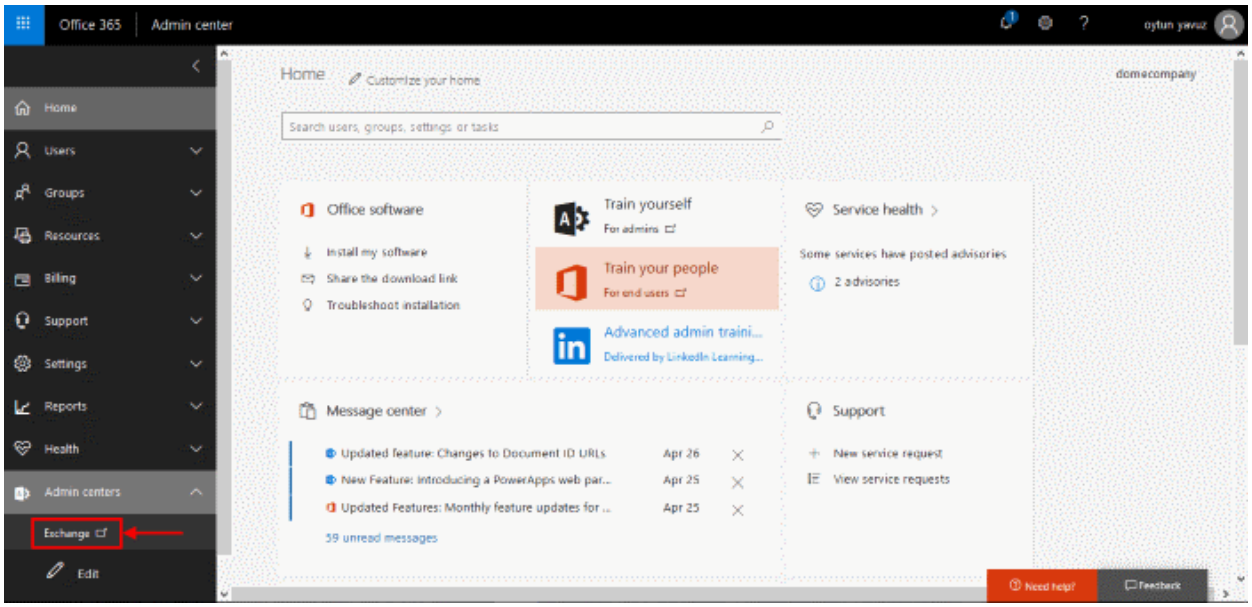
- Click 'Save' after you receive the success message:



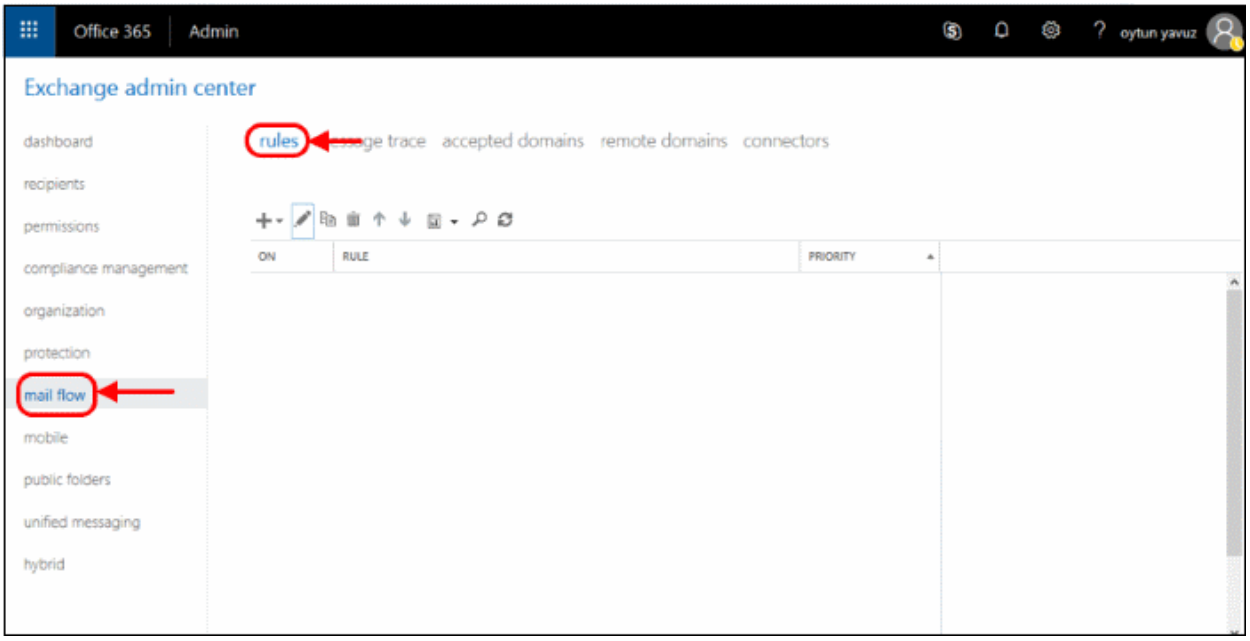
3.2.1 Add an email flow rule to use the Korumail Outbound connector

To set up outbound flow set up on Office 365

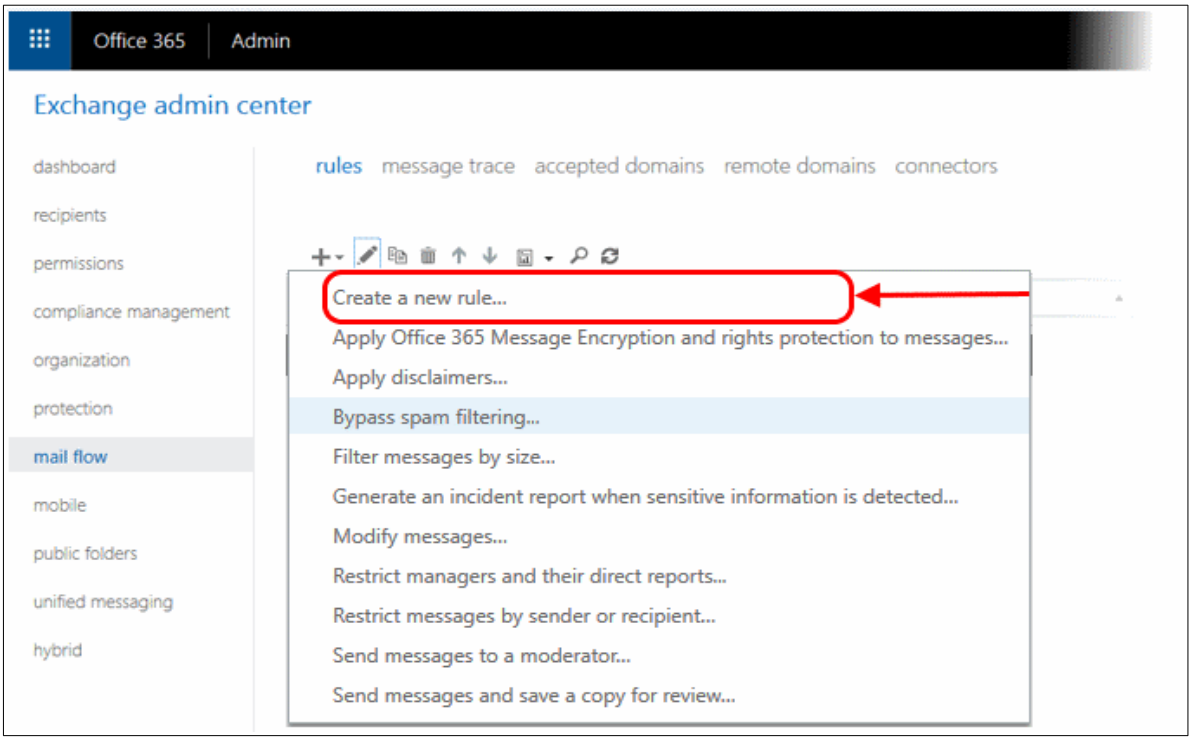
- Login to your Microsoft Office 365 administrator center account
  - Click 'Admin' in the left-hand menu
  - Click 'Admin' > 'Exchange':



- Click 'mail flow' on the left
- Click 'rules' in the top navigation:



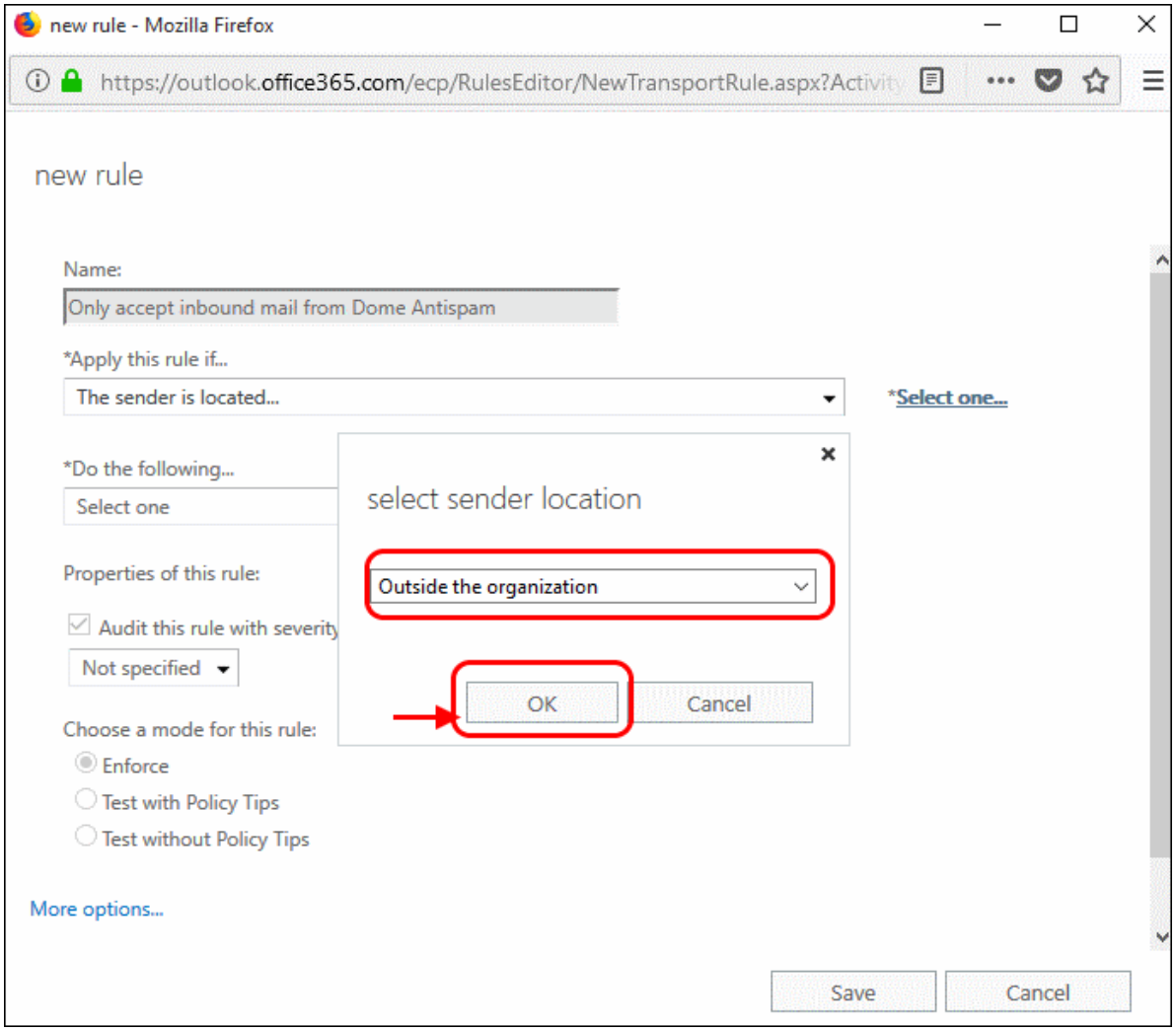
- To create a new rule:
  - Select 'Office 365' in 'From' drop-down menu
- Click the '+' sign and select 'Create a new rule...' from drop-down menu



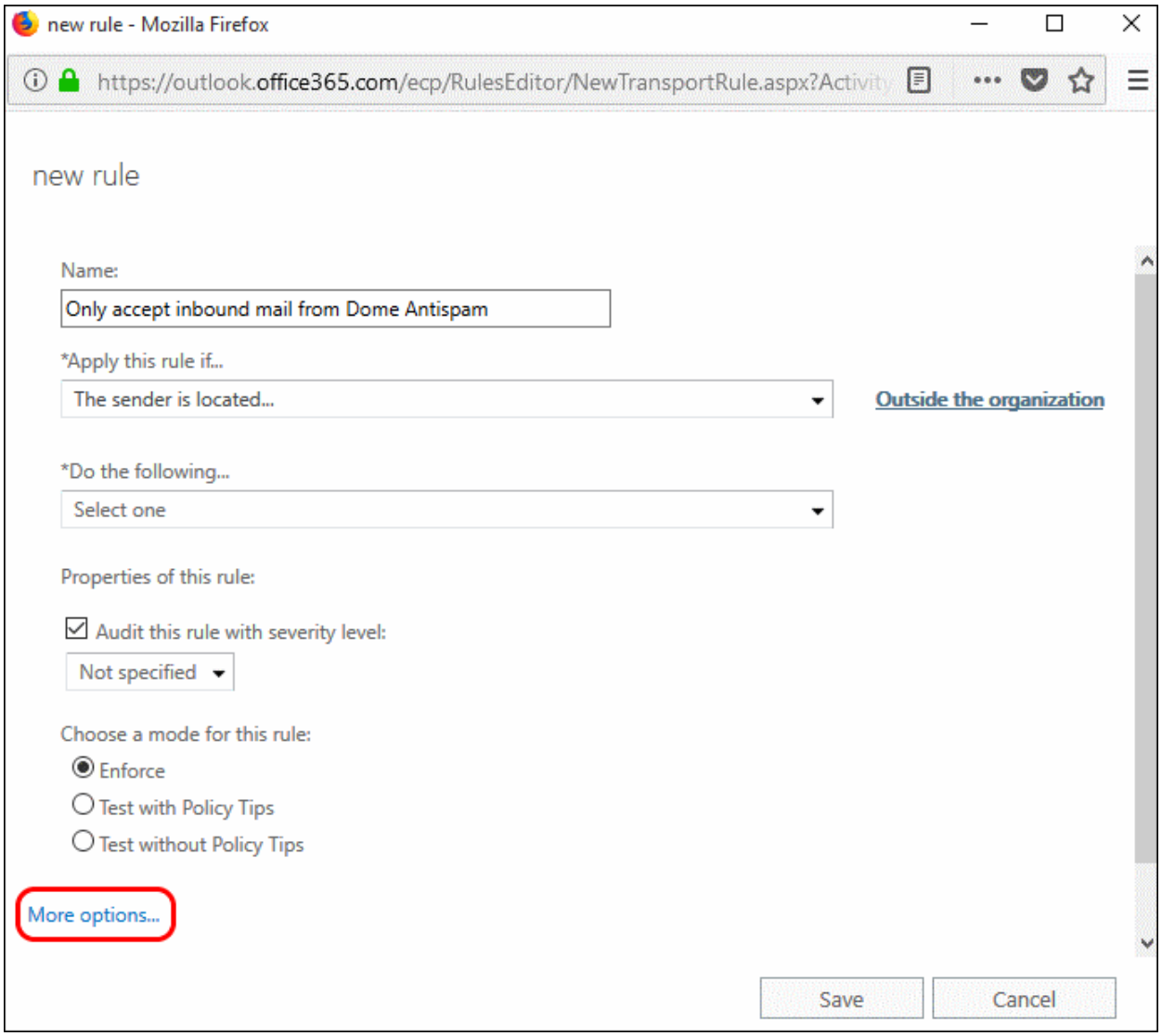
In the opening Rule window, enter:

- **Select the sender location** : Outside the organization
- **Apply this rule if..** : The sender is located
- This will open a pop-menu. Select 'Outside the organization' from the menu

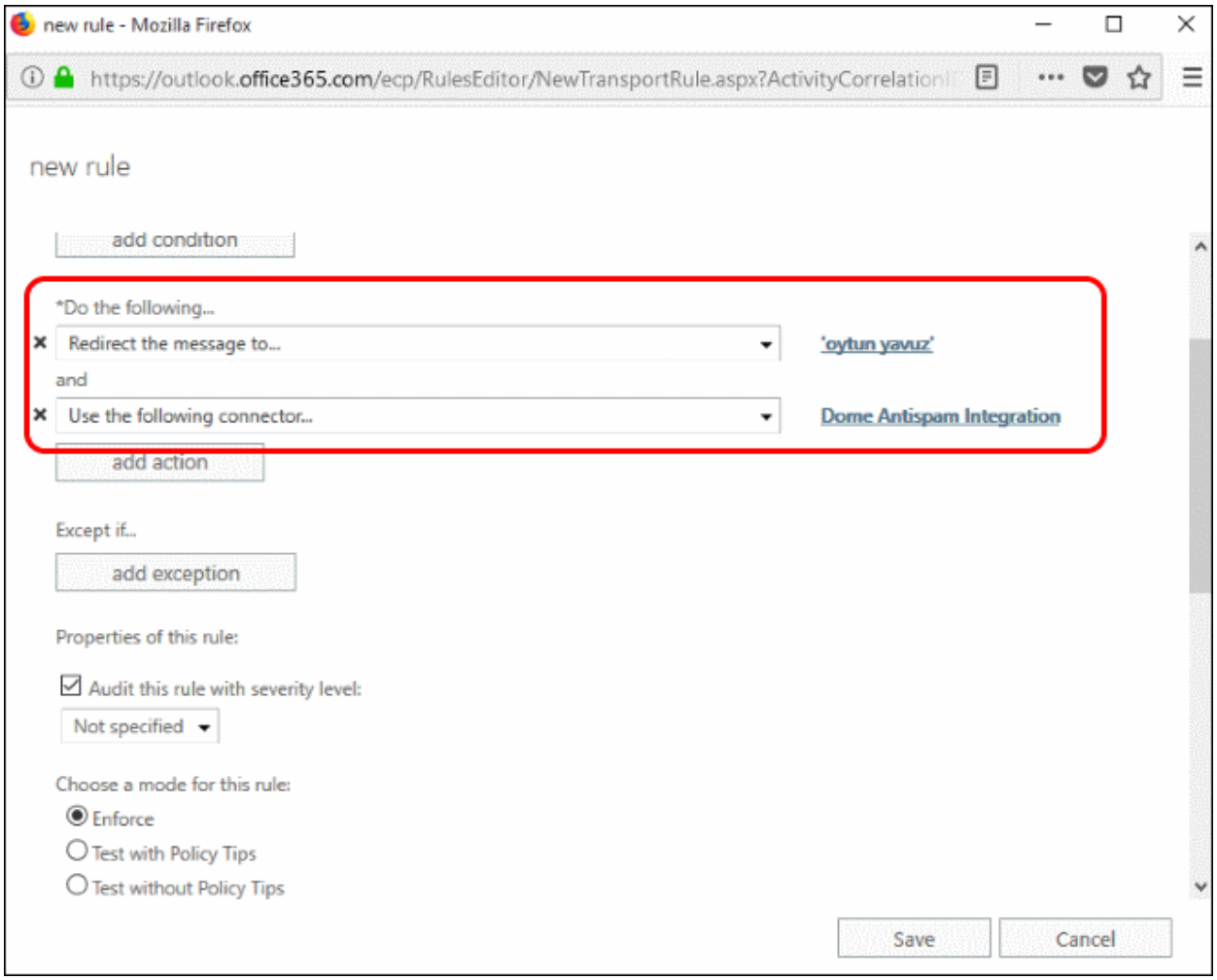
- Click 'OK':



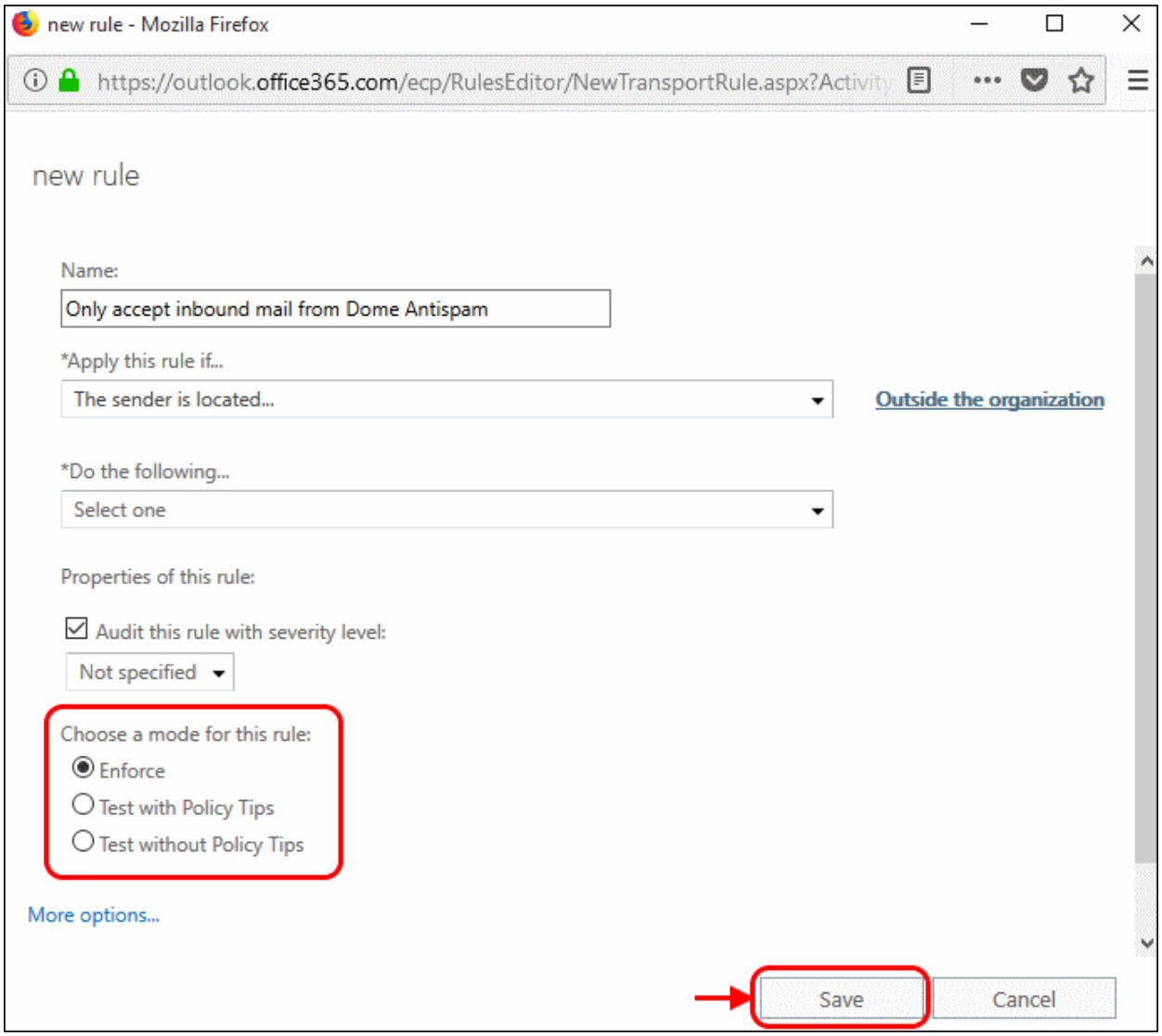
- Click 'More Options'



- Do the following :
  - Redirect message to a sender outside the organization
  - Select the outbound connector you created for Korumail



- Select 'Enforce' from 'Select the mode for this rule'


new rule - Mozilla Firefox
https://outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?Activity
new rule
Name:
Only accept inbound mail from Dome Antispam
*Apply this rule if...
The sender is located...
Outside the organization
*Do the following...
Select one
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...
Save
Cancel

- Click 'Save'

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**