myBUSINESS

Cyber Phishing Whitelisting Guide

myBUSINESS

Cyber Phishing Whitelisting Guide

Please ensure the following IP addresses are whitelisted in your email server:

104.130.122.237
159.135.224.107

My Business sends phishing simulations that replicate real-world attacks, and as such most mail filters will block the campaigns by default. **If you do not whitelist these IP addresses the phishing simulation emails will most likely go to spam and will not be delivered to your learners.**

Follow the **below guides for Office 365 (pages 8-31) and G-Suite/Gmail (pages 2-7)** to whitelist these addresses.

We recommend setting up a test phishing campaign to yourself or a low volume sending group after you follow the below steps to ensure your whitelisting was successful.
The setting may take up to an hour to propagate to all users.

If you have an IT department or contractor simply email them with message or send them this guide.

Hi [name],

We are enrolling staff into regular phishing simulations and online security awareness training. It is important that these emails are delivered to the inbox of our staff. Please ensure the following IP are whitelisted for inbound delivery at our mail gateway.

104.130.122.237
159.135.224.107

If you do not have IT support, follow the **below guides for:**

- G-Suite/Gmail (pages 2-7)
- Office 365 (pages 8-31)

If you do not complete this step the phishing simulation emails will most likely go to spam and will not be delivered to your learners.

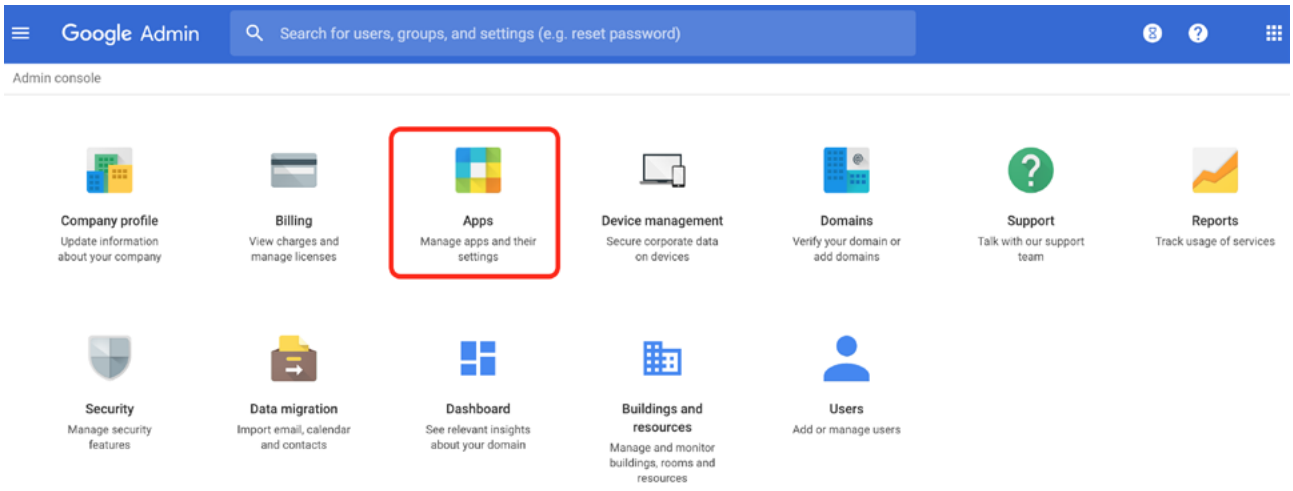
SECTION 1:
Gmail/G Suite/Google Apps

The guide below will assist in the process of whitelisting the security portal to ensure accurate delivery and reporting of campaigns sent to GSuite and Google Apps accounts.

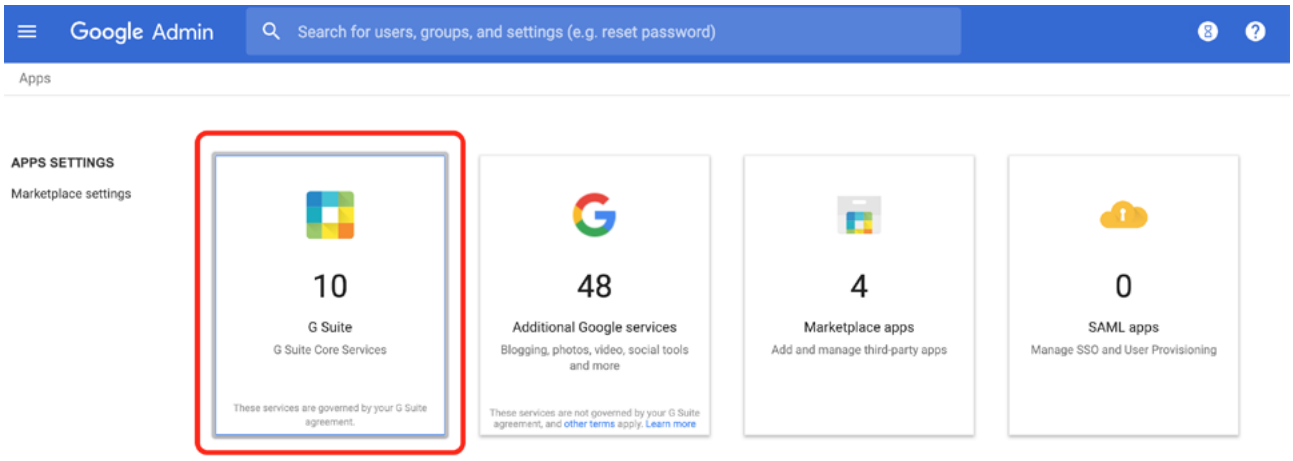
We recommend setting up a test phishing campaign to yourself or a low volume sending group after you follow the below steps to ensure your whitelisting was successful.
The setting may take up to an hour to propagate to all users.

Part 1: Add Sending IP addresses to email whitelist

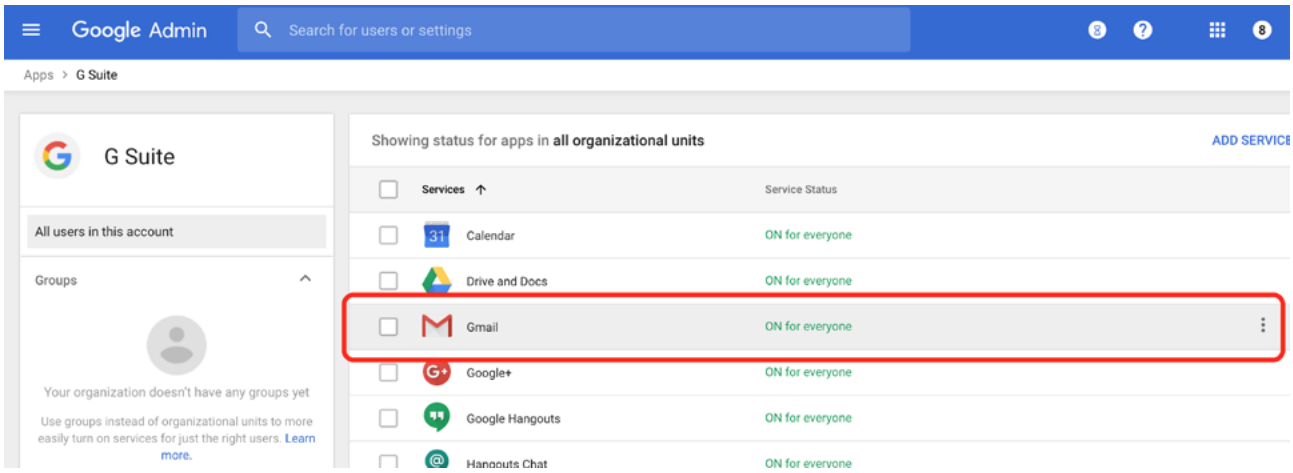
Log in to https://admin.google.com and select **Apps**



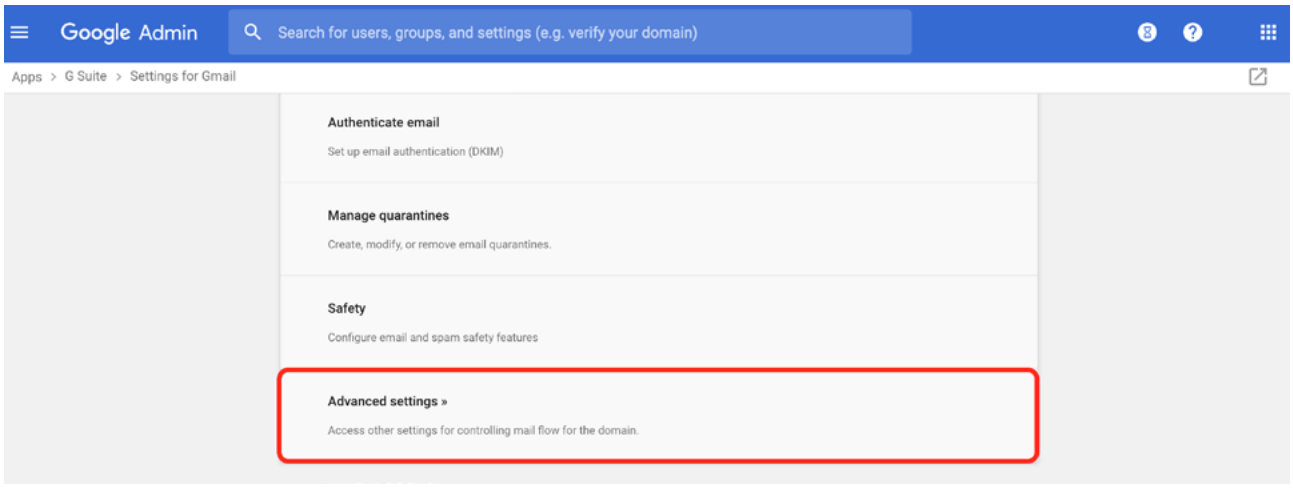
Select **G Suite**



Select **Gmail**

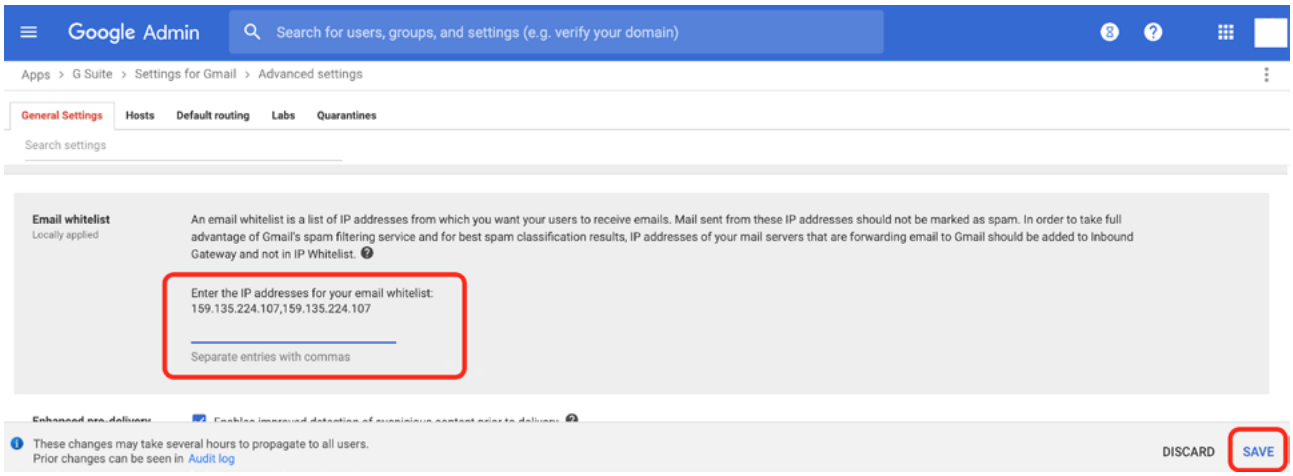


Select **Advanced Settings**



In the **Email whitelist** section, enter the following **IP addresses** separated by commas:

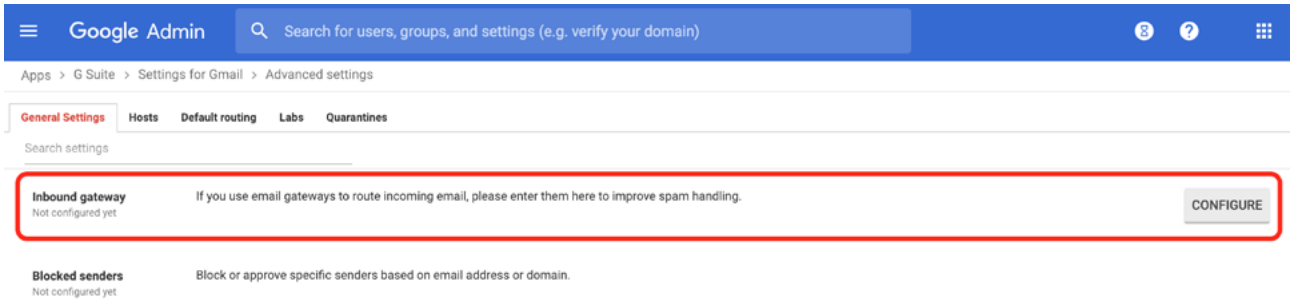
- 159.135.224.107
- 104.130.122.237



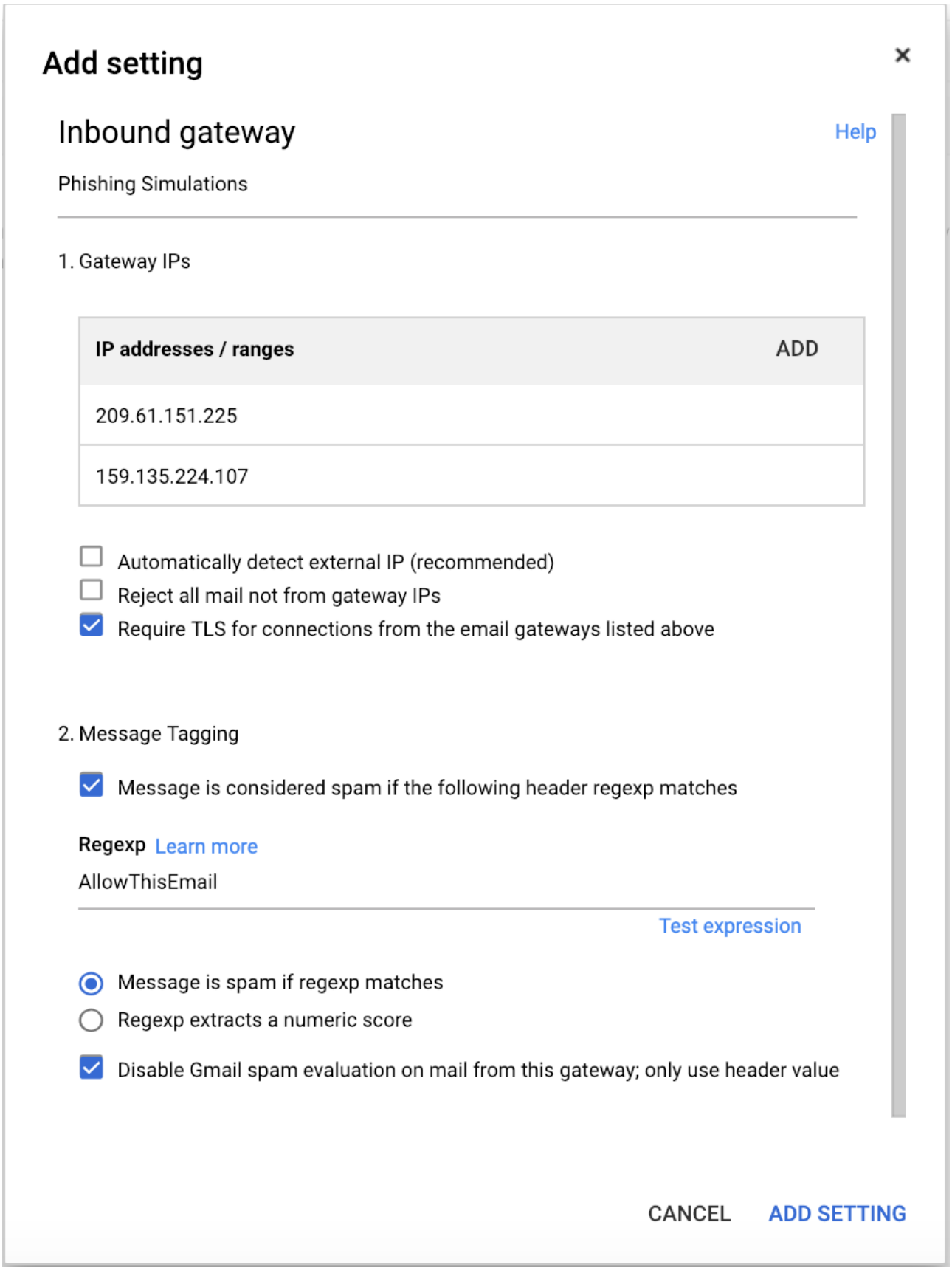
Part 2: Add IP addresses as Inbound Gateways

This method of whitelisting is to prevent the following Google banners from appearing in your user's inbox:

1. Log in to your Google Admin Console.
2. Navigate to **Apps** > **GSuite** > **Gmail** > **Advanced Settings**.
3. Scroll down to the **Inbound Gateway** setting located under the **Spam** section. Hoverover the setting and click the **Edit** button. This will open the **Inbound gateway** screen.



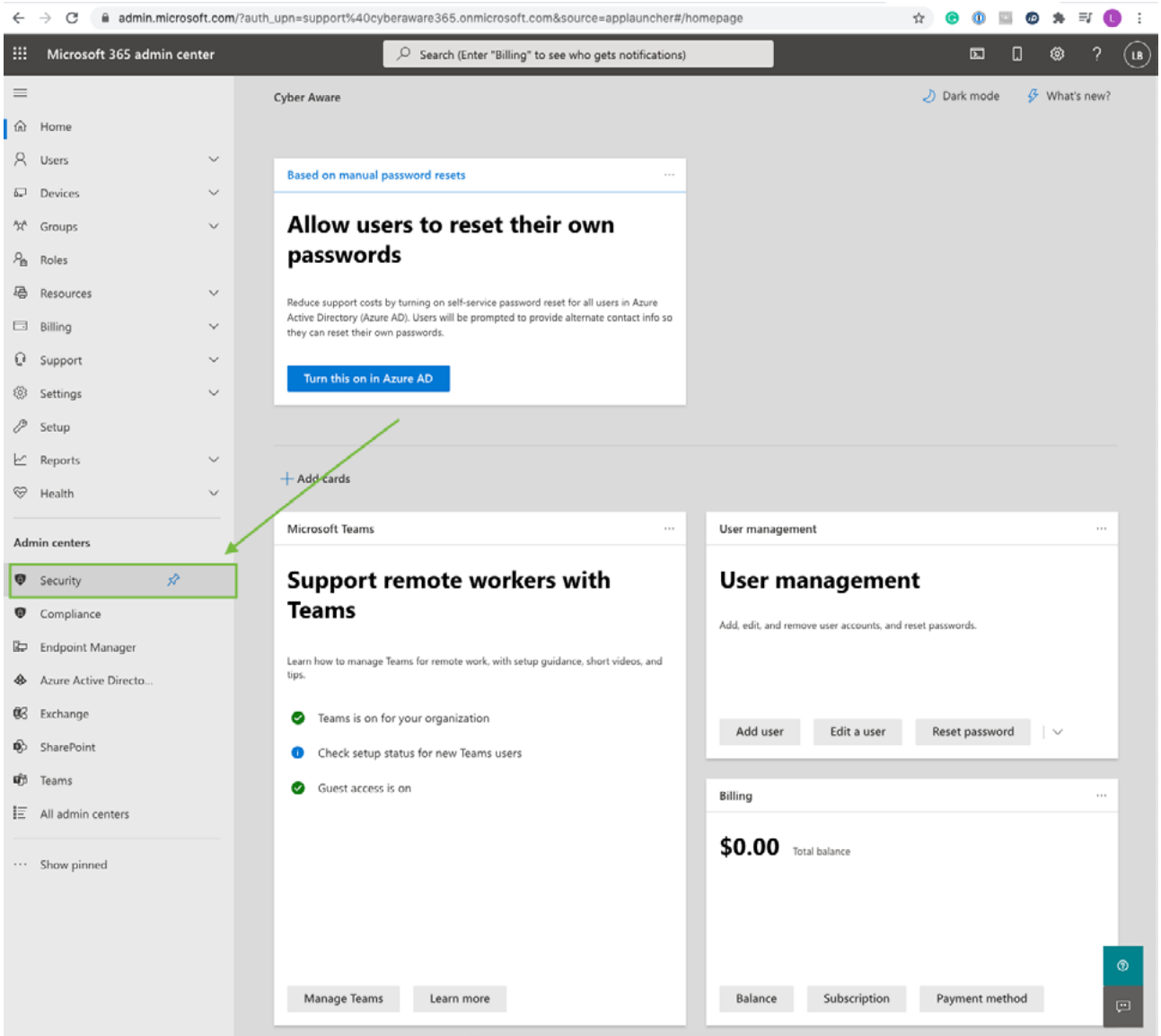
Configure the **Inbound gateway** using the settings below:


Add setting
Inbound gateway
Help
Phishing Simulations
1. Gateway IPs
IP addresses / ranges
ADD
209.61.151.225
159.135.224.107
Automatically detect external IP (recommended)
Reject all mail not from gateway IPs
Require TLS for connections from the email gateways listed above
2. Message Tagging
Message is considered spam if the following header regexp matches
Regexp Learn more
AllowThisEmail
Test expression
Message is spam if regexp matches
Regexp extracts a numeric score
Disable Gmail spam evaluation on mail from this gateway; only use header value
CANCEL
ADD SETTING

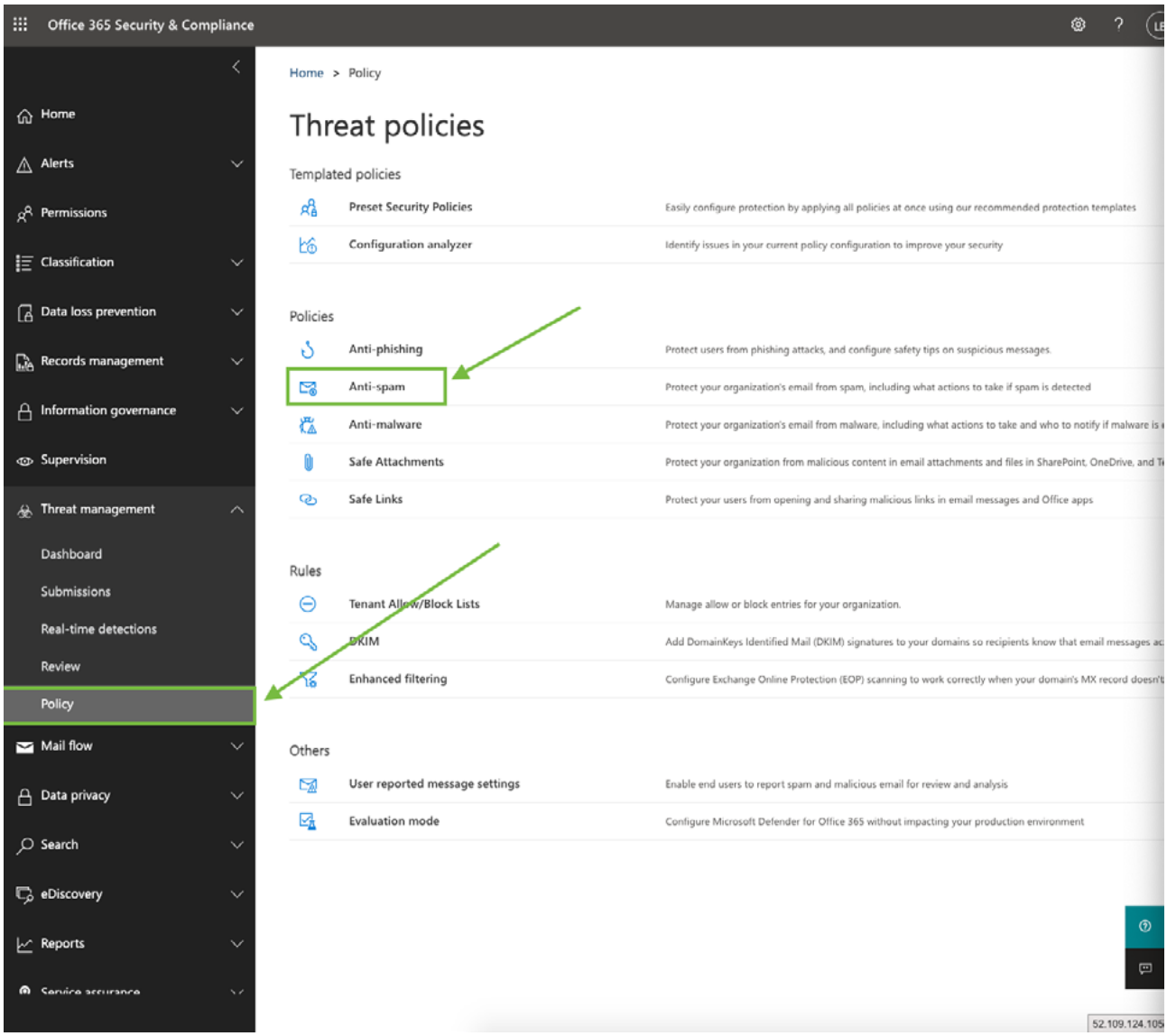
1. **Gateway IPs**
   Add the IP Addresses for:
   - 159.135.224.107
   - 104.130.122.237
2. Leave the **Reject all mail not from gateway IPs** option unchecked
3. Check **Require TLS for connections from the email gateways listed above**
4. **Message Tagging**
   Enter text "**AllowThisEmail**" for the **Spam Header Tag**
5. Select the **Disable Gmail spam evaluation on mail from this gateway; only useheader value**
6. Click the **ADD SETTING** button

SECTION 2:
Office 365 Instructions

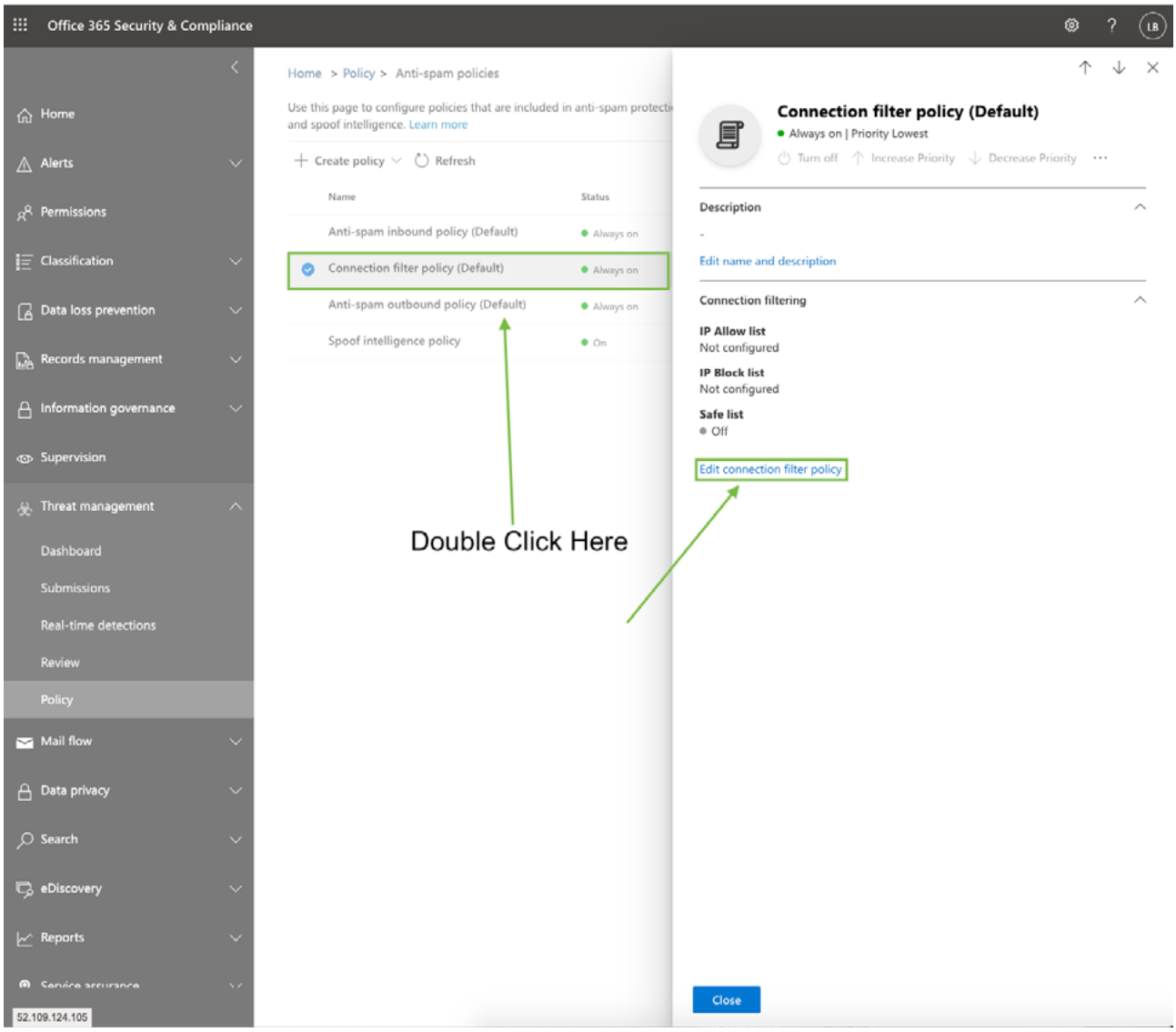
1. Log in to Office 365 and go to **Security**



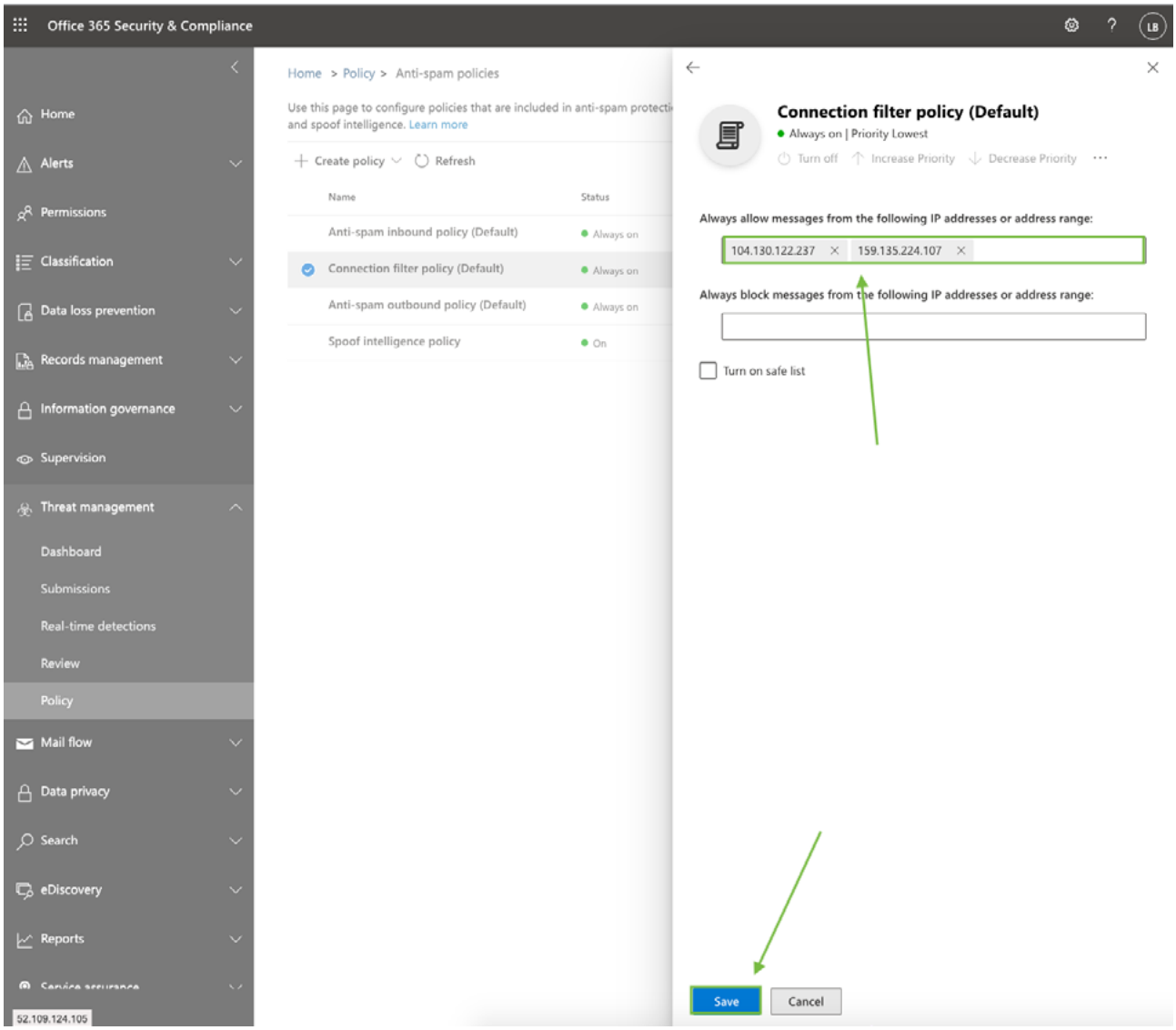
2. Go to **Policy** > **Anti-spam**



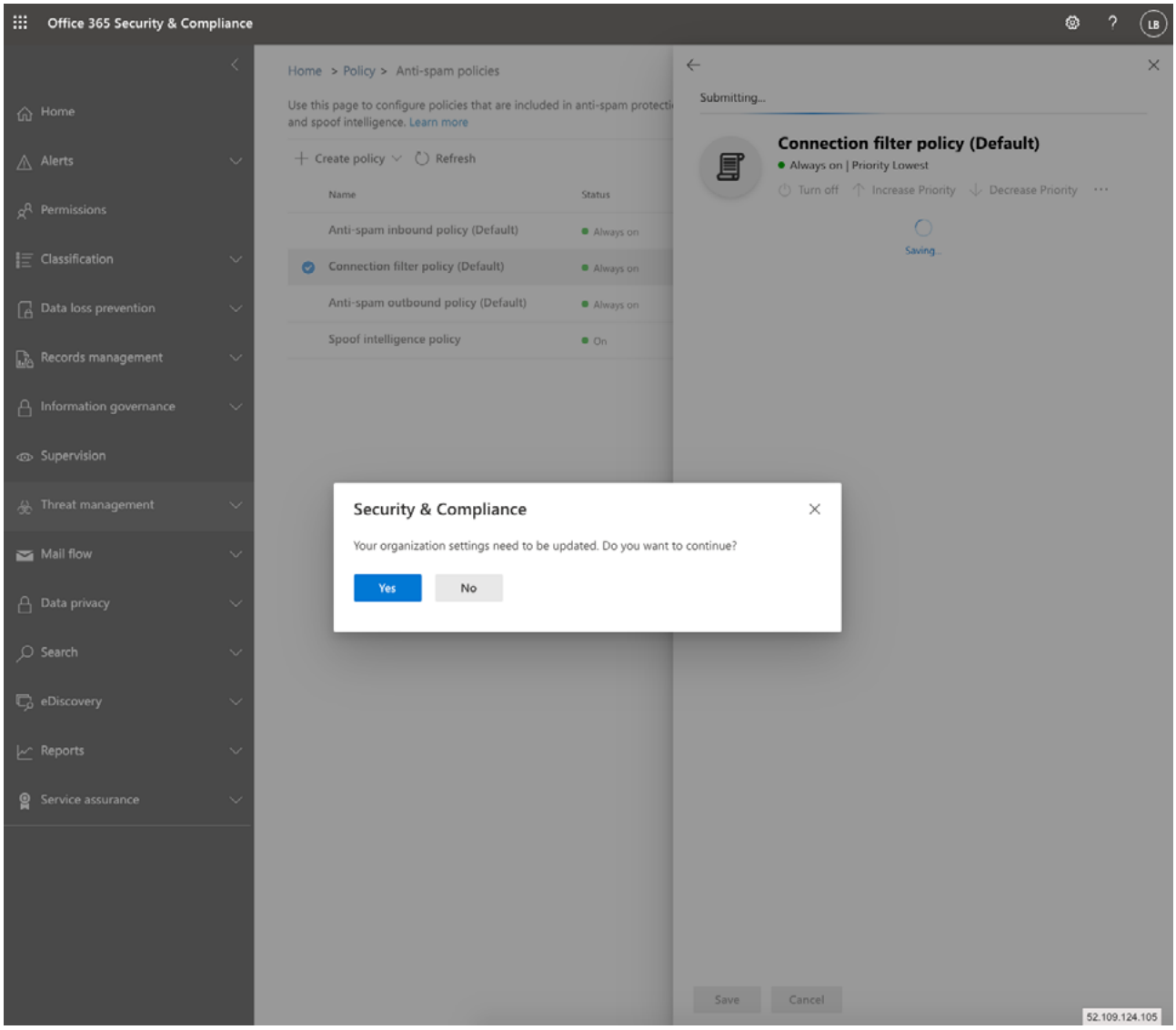
3. Double click '**Connection Filter Policy**' > Click **Edit Connection Filter Policy**



4. Enter the following IP Addresses then click **Save**:
   a. 104.130.122.237
   b. 159.135.224.107

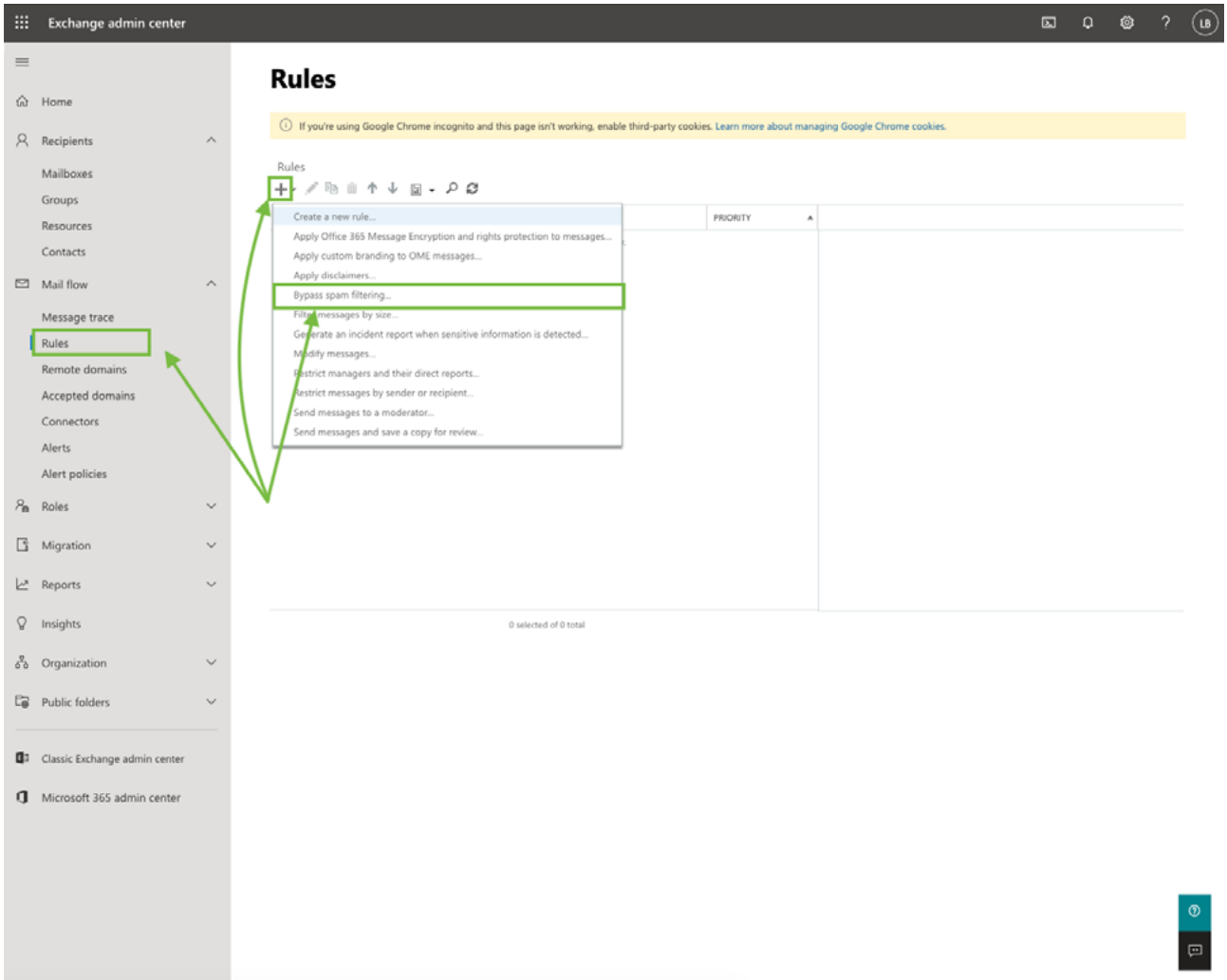


5. If the following prompt pops up, click **Yes**

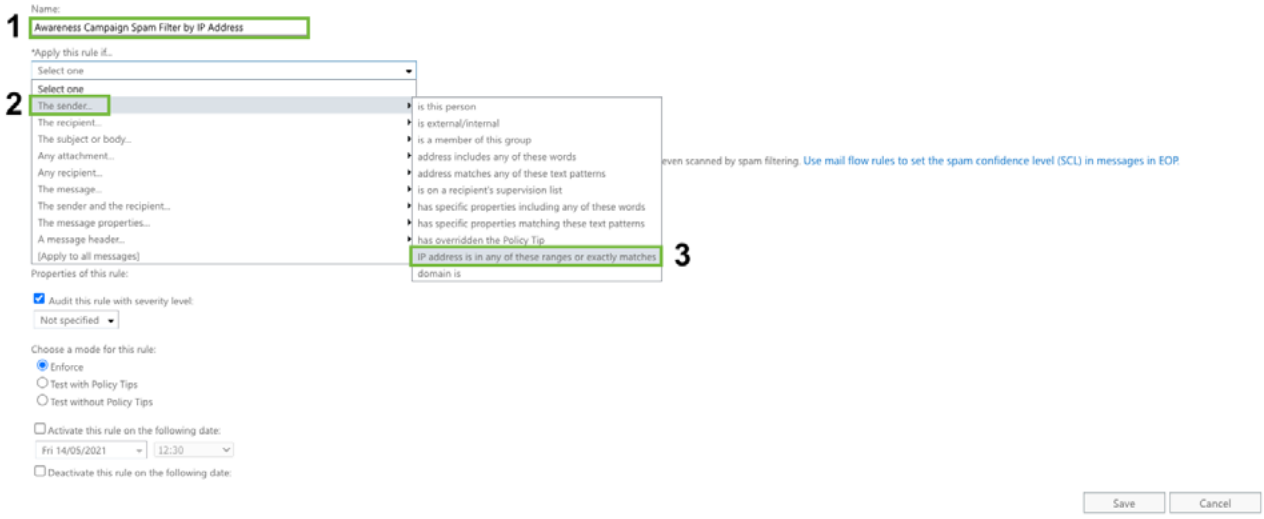


Add Mail Flow rules to bypass spam filtering and clutter

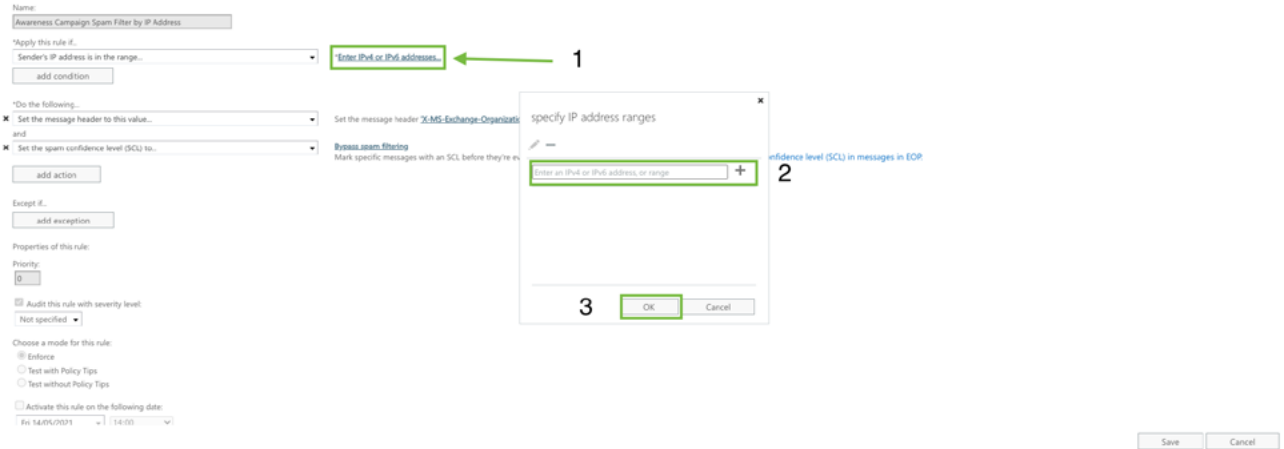
1. Go to your **Exchange admin centre**
    a. This can be found via the following URL: https://admin.exchange.microsoft.com
2. Go to **Mail Flow** > **Rules**
    a. Create a Bypass Spam Filtering Rule



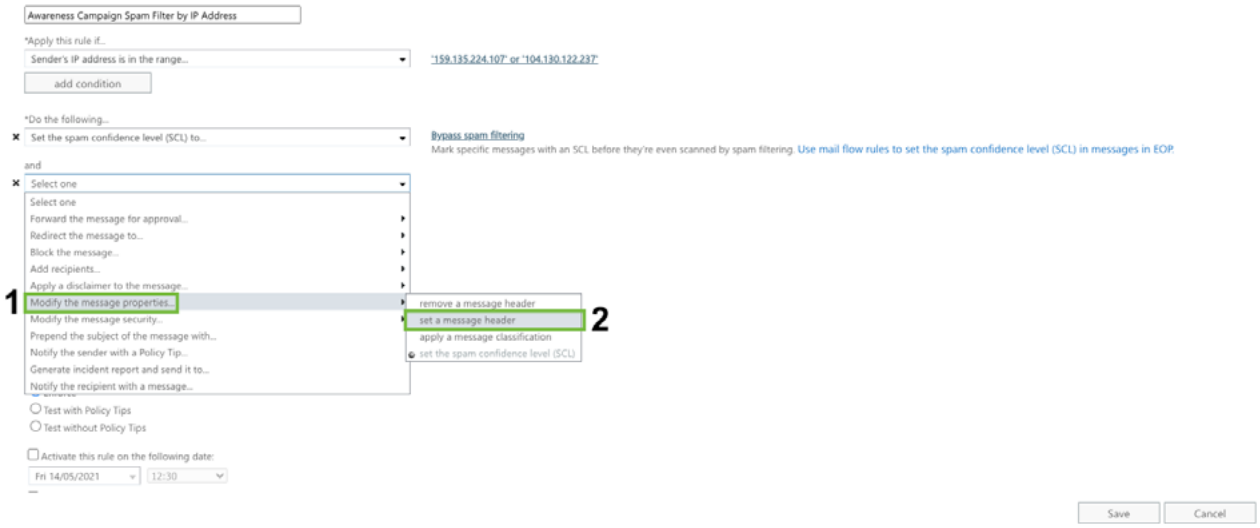
3. Fill in the following details
   a. **Name:** *Awareness Campaign Spam Filter by IP Address*
   b. **Apply this rule if:** *The sender IP address is any of these ranges or exactly matches*



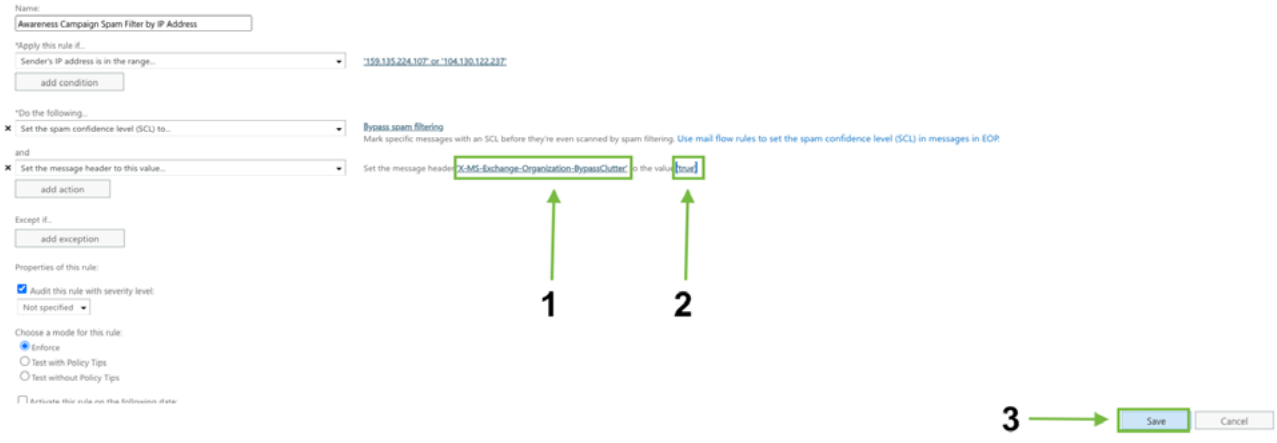
4. Click "**Enter IPv4 or IPv6 addresses...**" and enter
   a. 104.130.122.237
   b. 159.135.224.107



5. Add a **message header**
   a. Click **Add Actionb**
   b. Click '**Modify the message properties**' > '**Set a Message Header**'

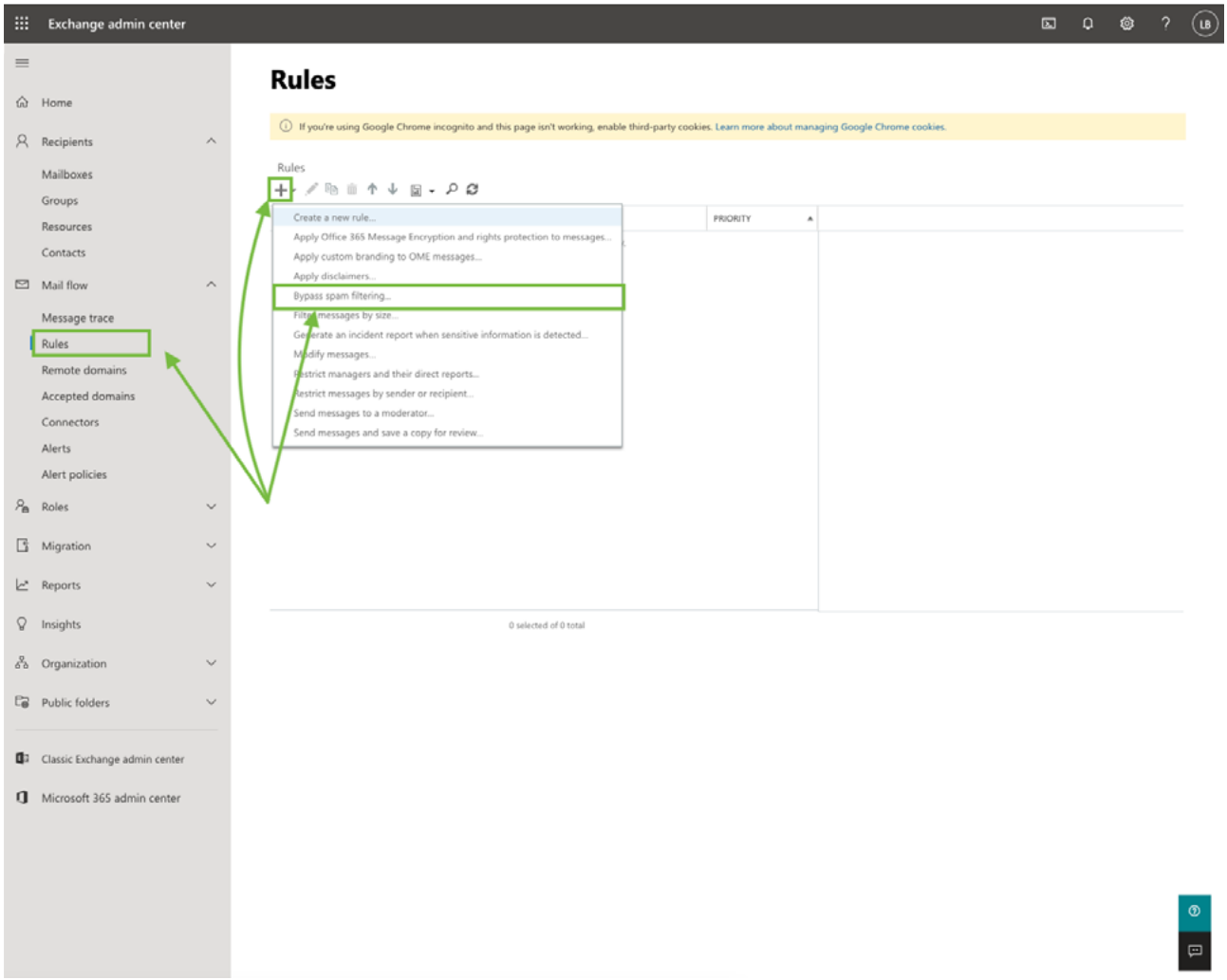


6. Modify the message header and value:
   a. Click on Set a message header "**Enter text…**" and add the following (case sensitive!):
      a. X-MS-Exchange-Organization-BypassClutter
   b. Click on … to the value "**Enter text…**" and add (case sensitive!):
      a. true
   c. Click **Save**

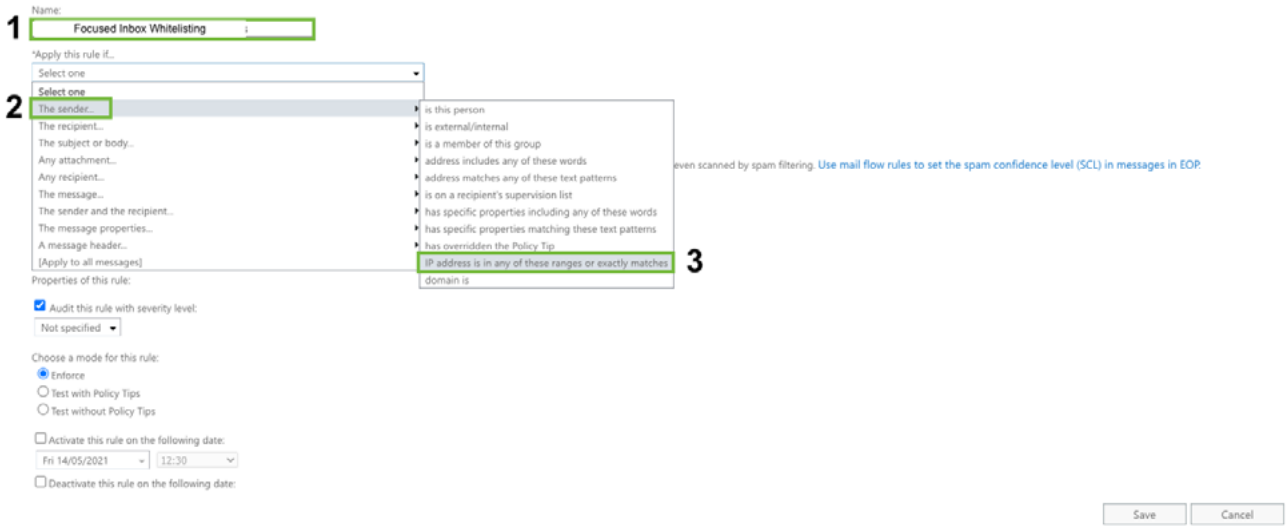


Add Mail Flow Rule to bypass focused inbox

1. Go to **Mail Flow** > **Rules**
    a. Create a Bypass Spam Filtering Rule

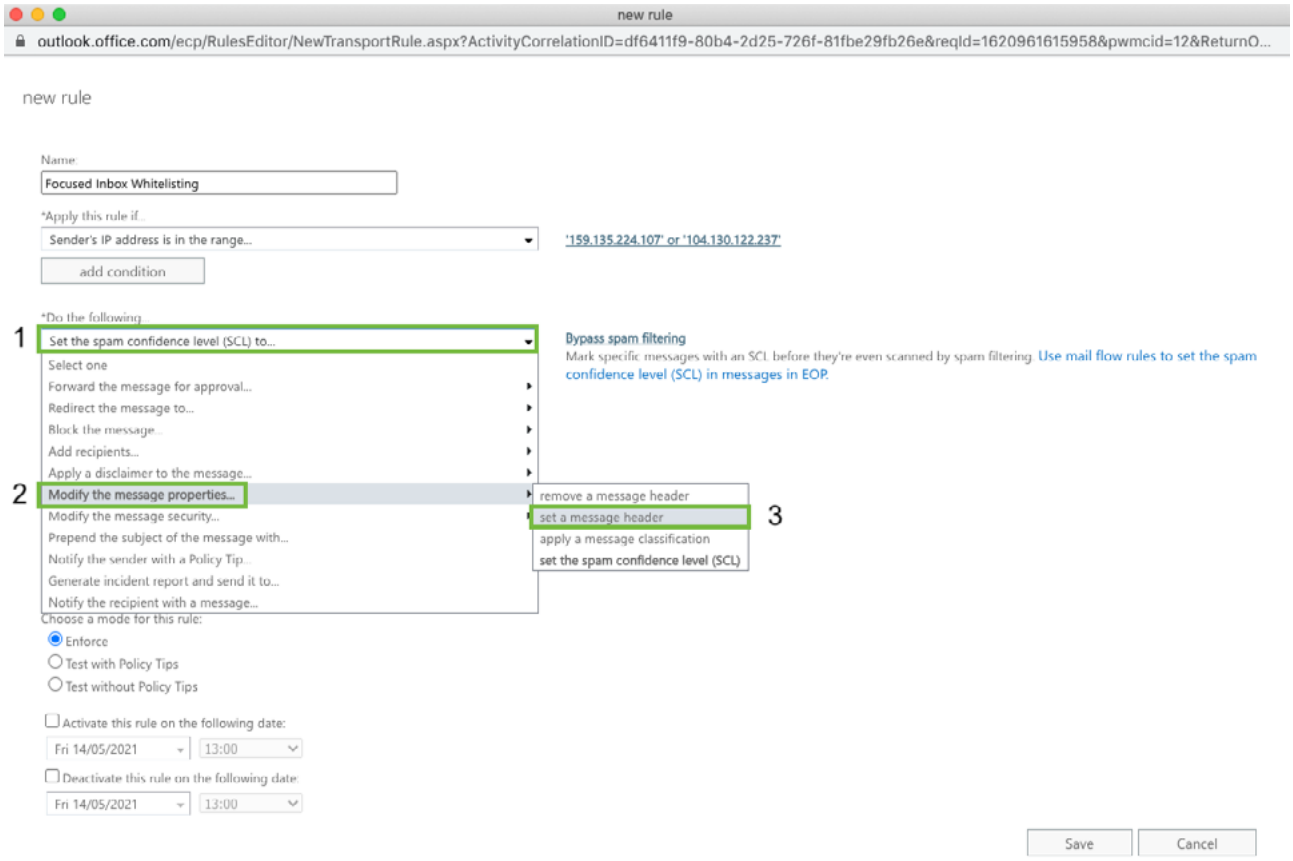


2. Fill in the following details
    a. **Name:** *Focused Inbox Whitelisting*
    b. **Apply this rule if:** *The sender IP address is any of these ranges or exactly matches*



3. Click "**Enter IPv4 or IPv6 addresses...**" and enter
    a. 104.130.122.237
    b. 159.135.224.107

4. Replace the Bypass Spam Filtering Rule:
   a. Click ***Do the Following….**
   b. Modify the **message properties** > set a message header



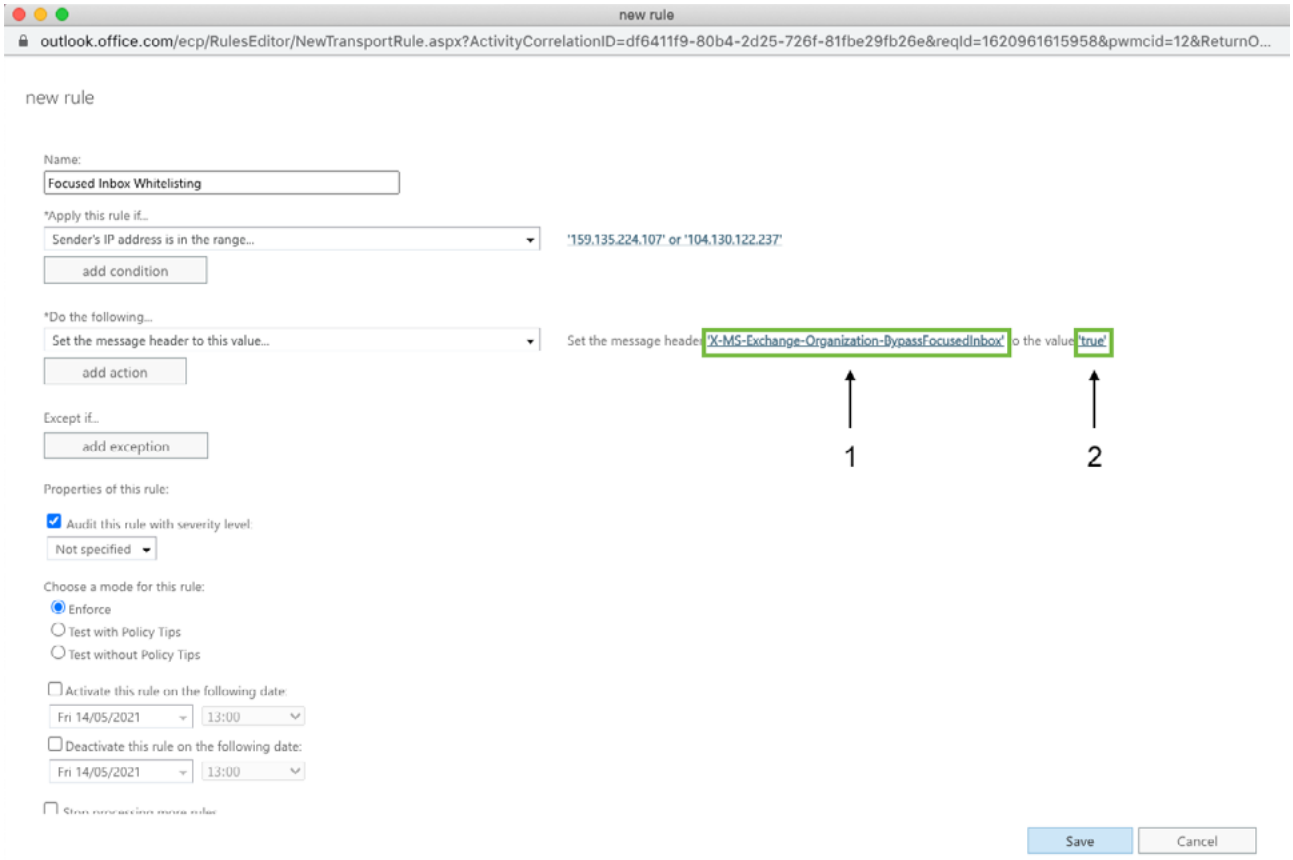
5. Modify the message header and value:

   a. Click on Set a message header "**Enter text…**" and add the following (case sensitive!):

      a. X-MS-Exchange-Organization-BypassFocusedInbox

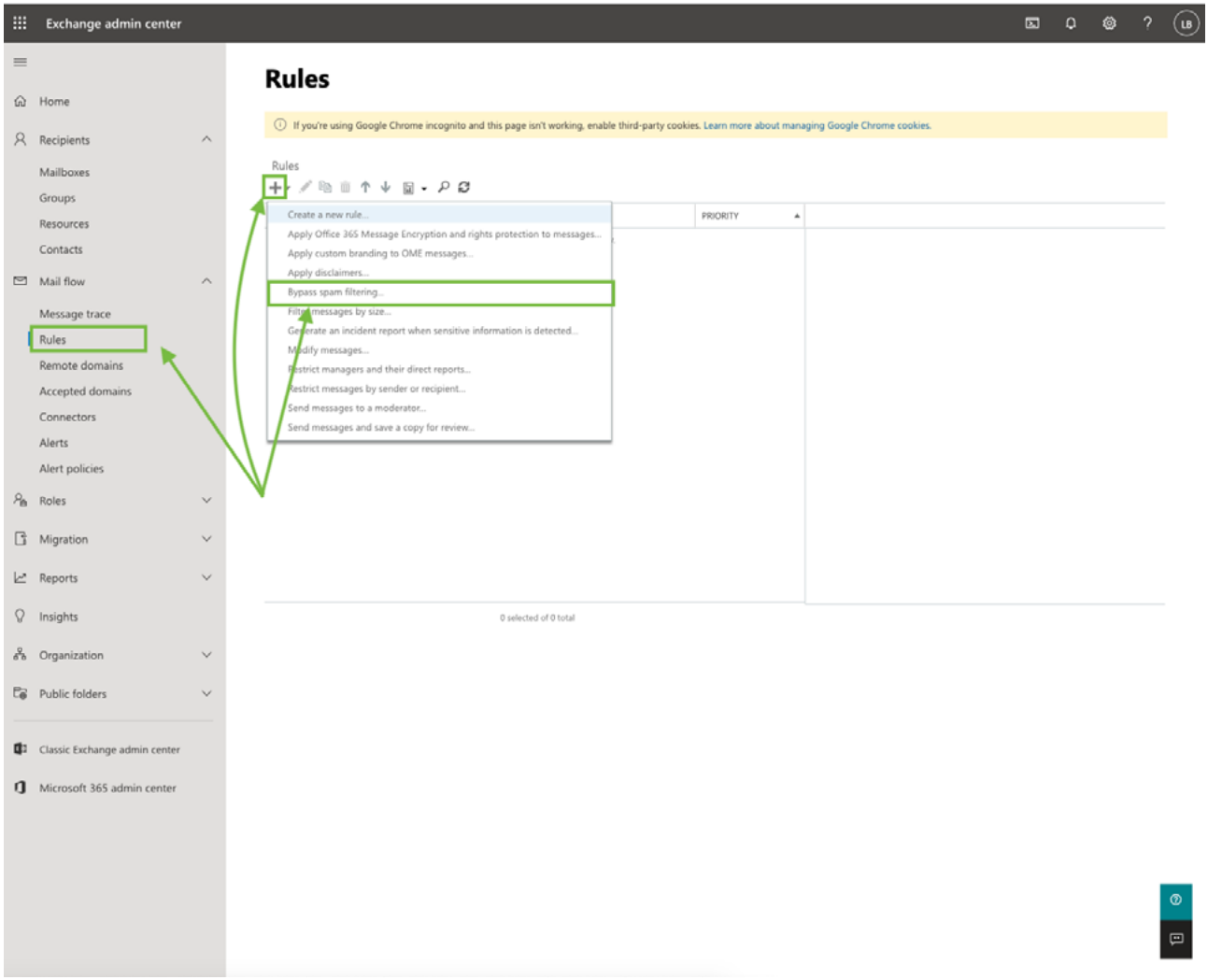
   b. Click on … to the value "**Enter text…**" and add (case sensitive!):

      a. true

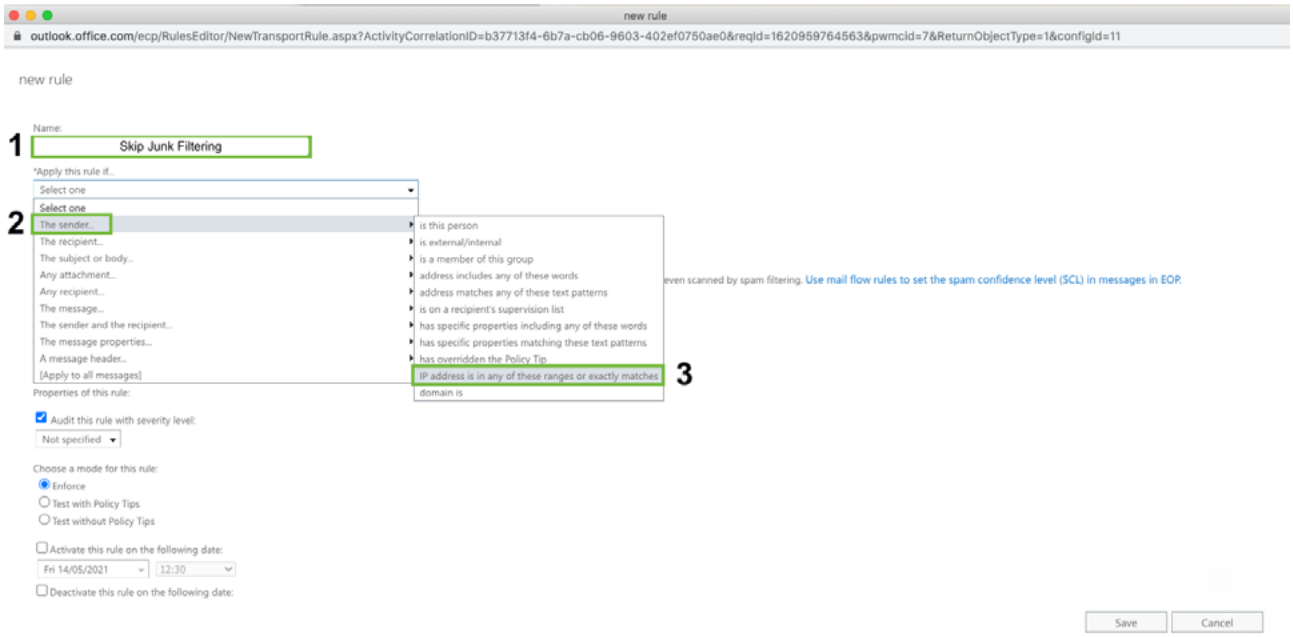


Add Mail Flow rule to skip junk filtering

1. Go to **Mail Flow** > **Rules**
    a. Create a Bypass Spam Filtering Rule

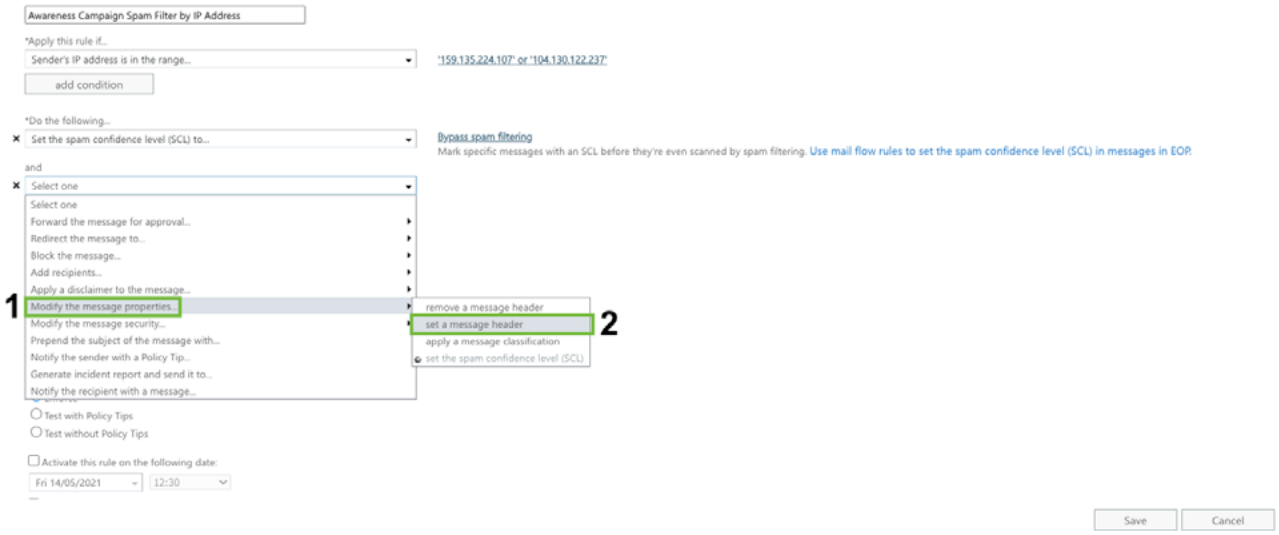


2. Fill in the following details
    a. **Name:** *Skip Junk Filtering*
    b. **Apply this rule if:** *The sender IP address is any of these ranges or exactly matches*



3. Click "**Enter IPv4 or IPv6 addresses...**" and enter
    a. 104.130.122.237
    b. 159.135.224.107

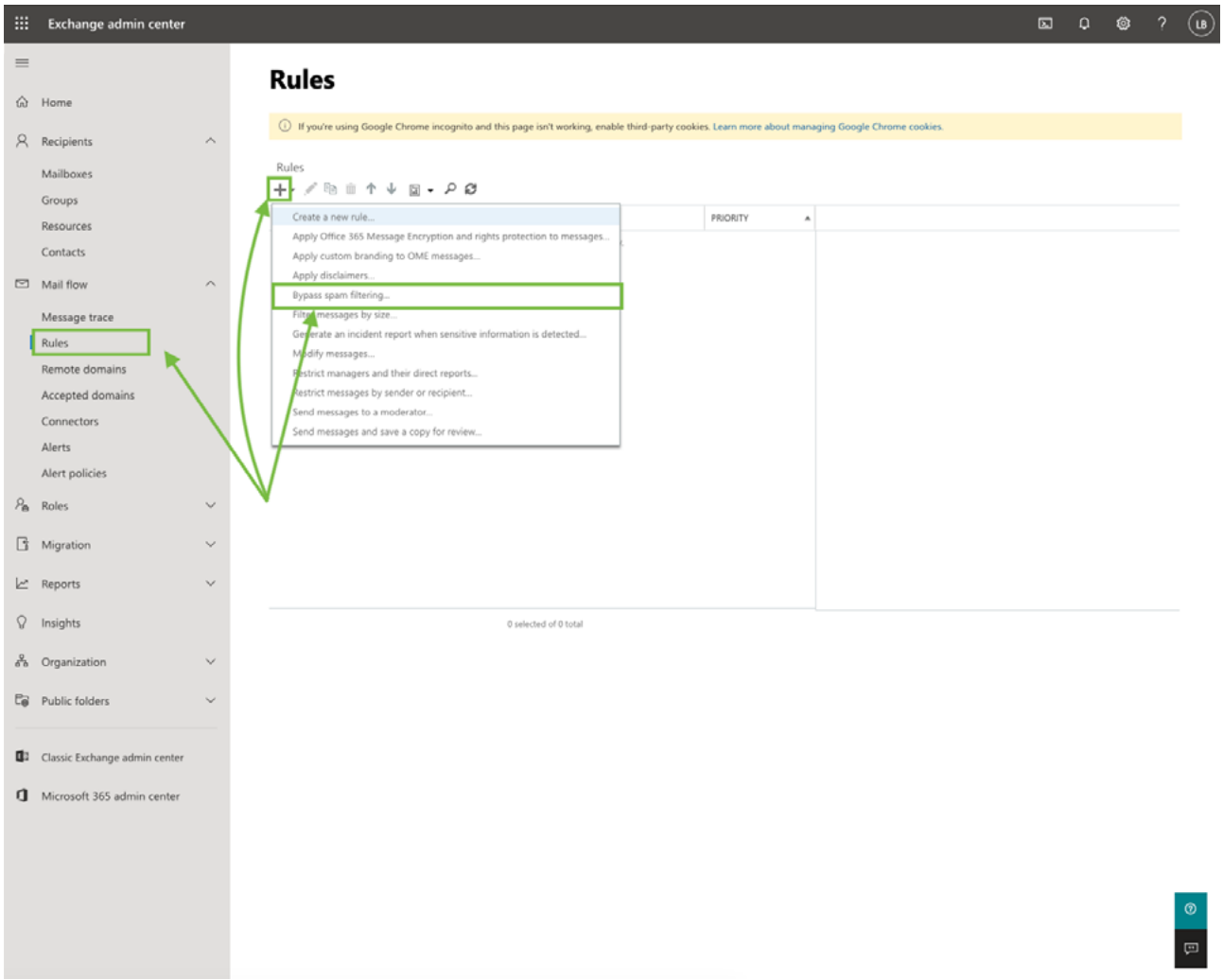
4. Replace the Bypass Spam Filtering Rule:
   a. Click ***Do the Following….**
   b. Modify the **message properties** > set a message header



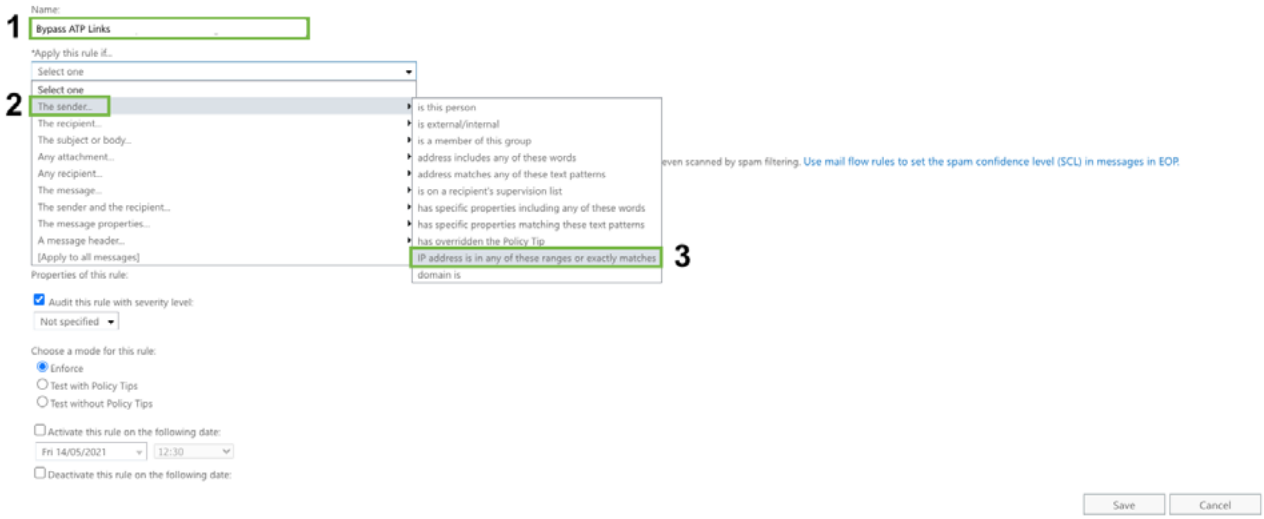
5. Modify the message header and value:
   a. Click on Set a message header "**Enter text…**" and add the following (case sensitive!):
      a. X-Forefront-Antispam-Report
   b. Click on … to the value "**Enter text…**" and add (case sensitive!):
      a. SFV:SKI;

ATP: Skip Link Scanning

1. Go to **Mail Flow** > **Rules**
    a. Create a Bypass Spam Filtering Rule

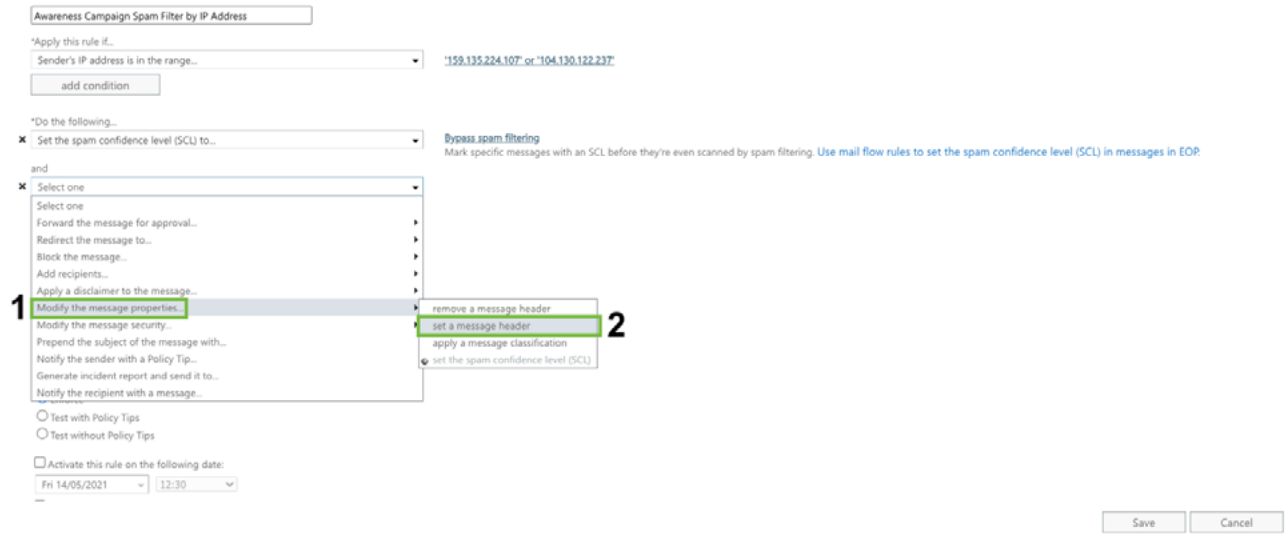


2. Fill in the following details
   a. **Name:** *Bypass ATP Links*
   b. **Apply this rule if:** *The sender IP address is any of these ranges or exactly matches*

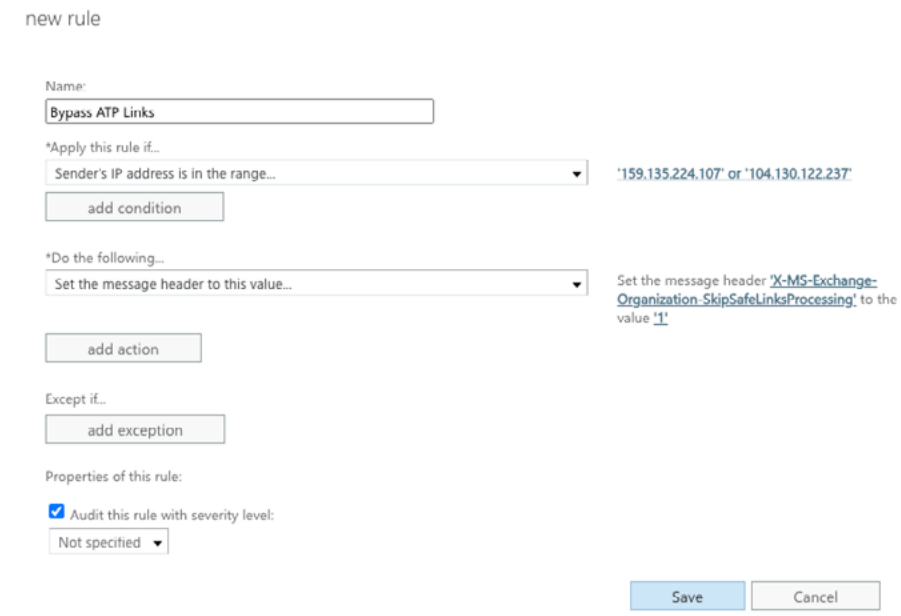


3. Click "**Enter IPv4 or IPv6 addresses...**" and enter
   a. 104.130.122.237
   b. 159.135.224.107

4. Replace the Bypass Spam Filtering Rule:
   a. Click ***Do the Following….**
   b. Modify the **message properties** > set a message header

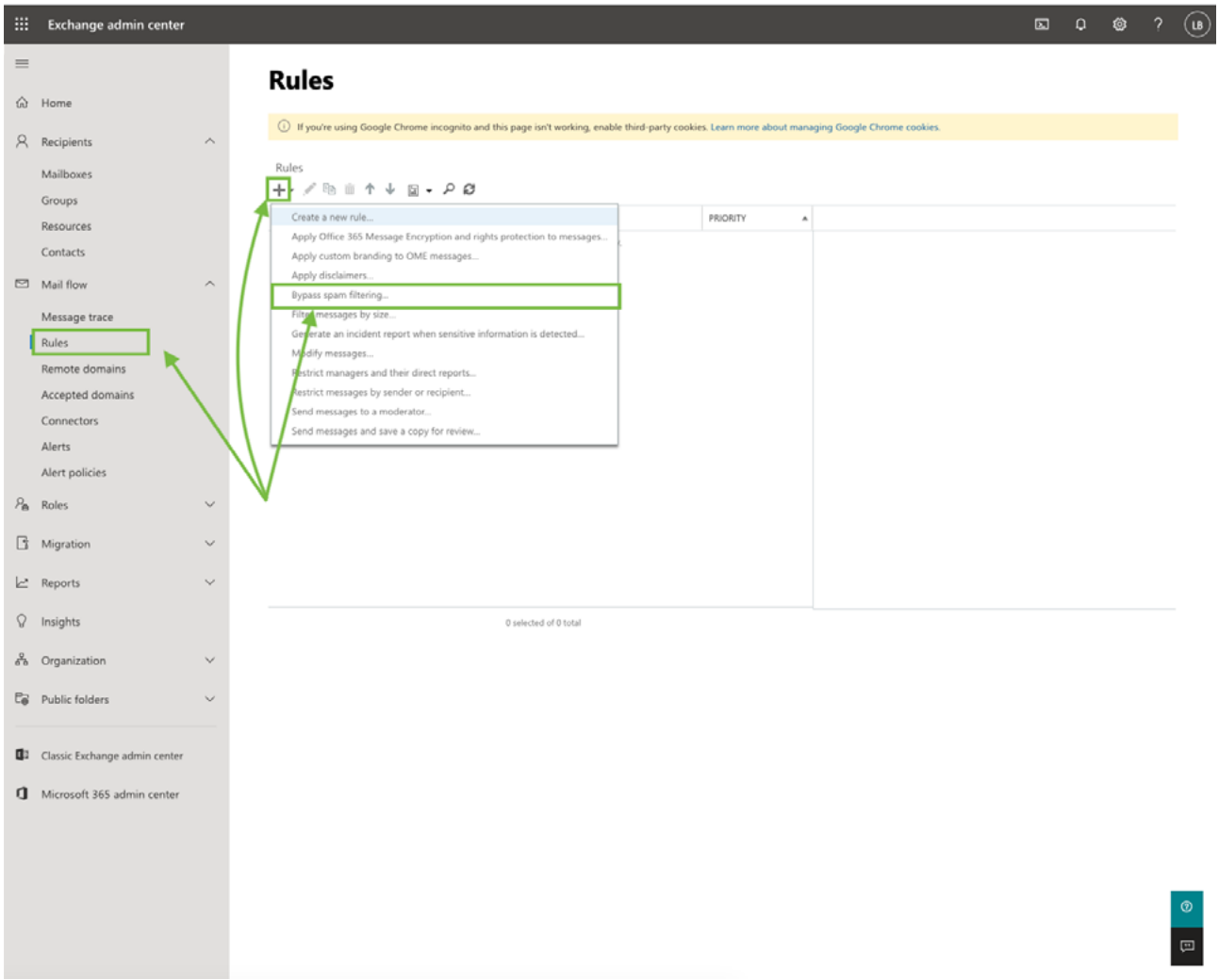


5. Modify the message header and value:
   a. Click on Set a message header "**Enter text…**" and add the following (case sensitive!):
      a. X-MS-Exchange-Organization-SkipSafeLinksProcessing
   b. Click on … to the value "**Enter text…**" and add (case sensitive!):
      a. 1

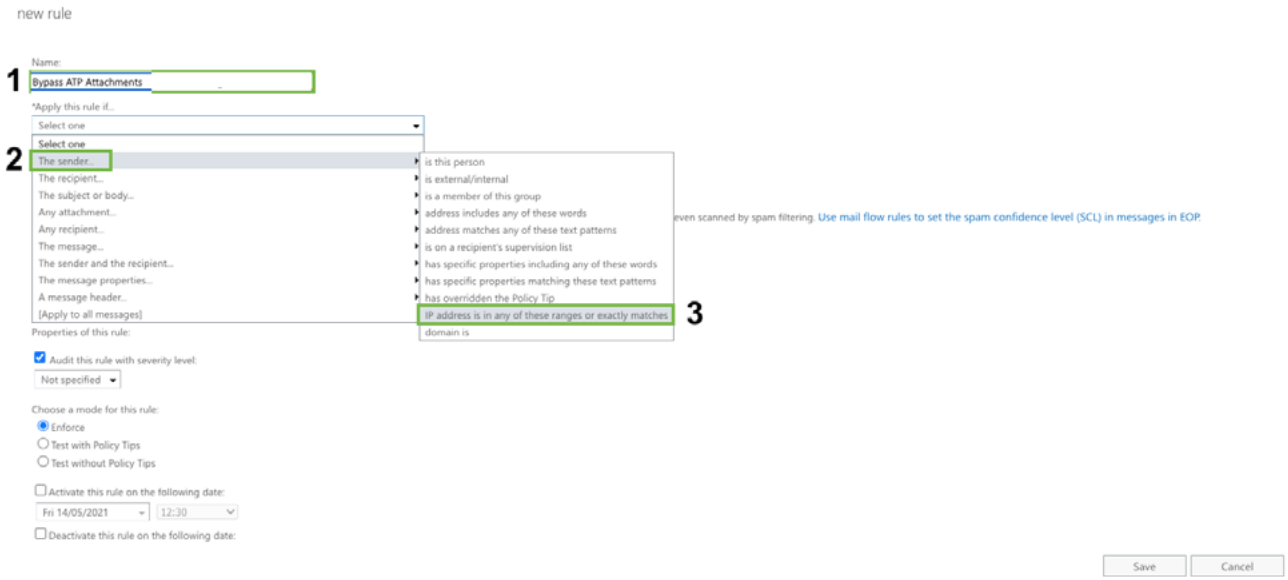


ATP: Skip attachment scanning

1. Go to **Mail Flow** > **Rules**
    a. Create a Bypass Spam Filtering Rule

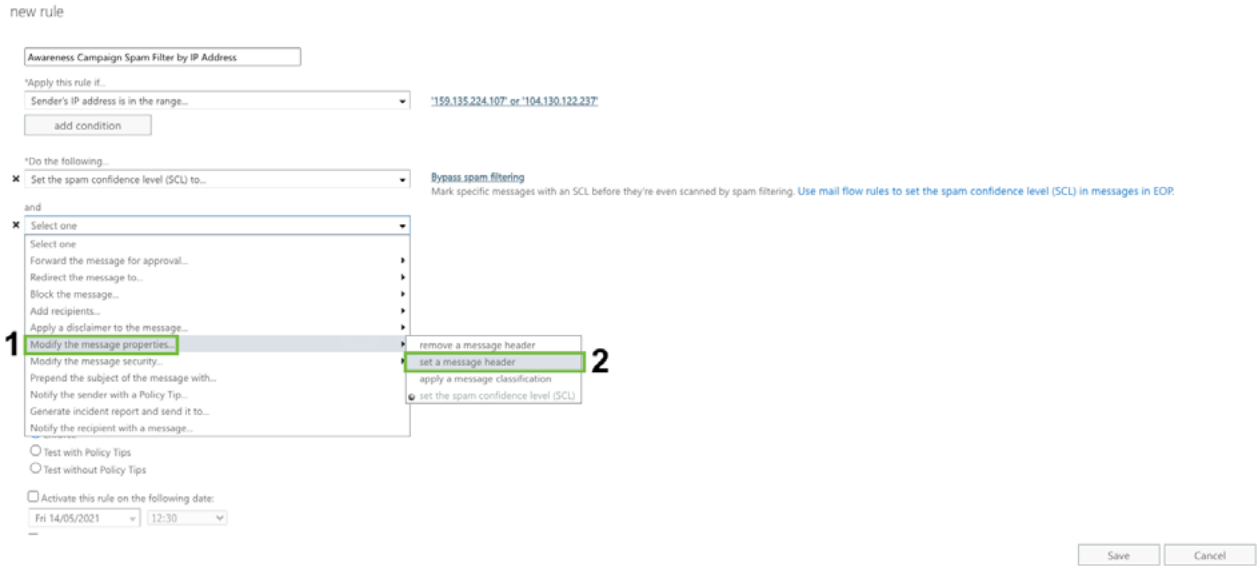


2. Fill in the following details
   a. **Name:** *Bypass ATP Attachments*
   b. **Apply this rule if:** *The sender IP address is any of these ranges or exactly matches*

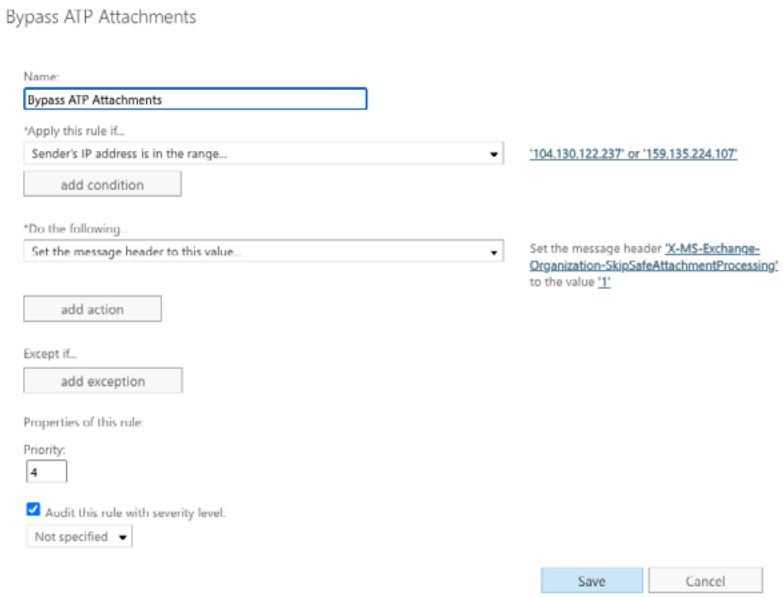


3. Click "**Enter IPv4 or IPv6 addresses...**" and enter
   a. 104.130.122.237
   b. 159.135.224.107

4. Replace the Bypass Spam Filtering Rule:
   a. Click ***Do the Following….**
   b. Modify the **message properties** > set a message header



5. Modify the message header and value:
   a. Click on Set a message header "**Enter text…**" and add the following (case sensitive!):
      a. X-MS-Exchange-Organization-SkipSafeAttachmentProcessing
   b. Click on … to the value "**Enter text…**" and add (case sensitive!):
      a. 1



Level 15, 140 Arthur Street, North Sydney NSW 2060
Tel 13 26 96 | contact@mybusiness.com.au | mybusiness.com.au
ABN 63 000 014 504