



Cyber Phishing Whitelisting Guide

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:

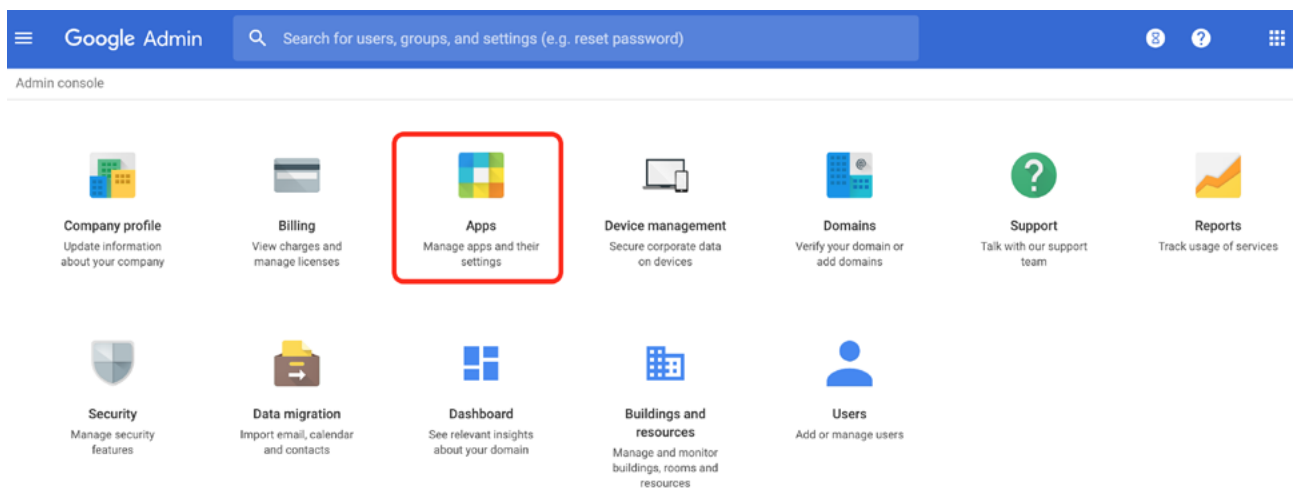
Gmail/G Suite/Google Apps

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

The screenshot shows the Google Admin console 'Apps' page. At the top, there is a search bar for users, groups, and settings. Below the search bar, there are four cards representing different app categories:

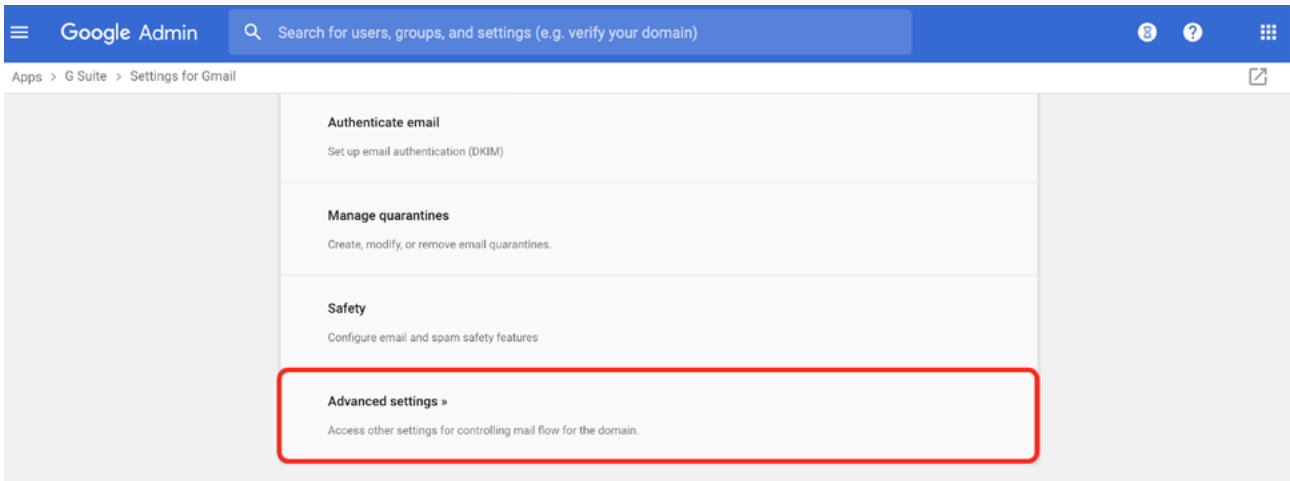
- G Suite**: 10 G Suite Core Services. This card is highlighted with a red box. Below the count, it says "These services are governed by your G Suite agreement."
- Additional Google services**: 48. Below the count, it says "These services are not governed by your G Suite agreement, and other terms apply. [Learn more](#)"
- Marketplace apps**: 4. Below the count, it says "Add and manage third-party apps"
- SAML apps**: 0. Below the count, it says "Manage SSO and User Provisioning"

Select Gmail

The screenshot shows the Google Admin console 'G Suite' page. On the left, there is a sidebar with 'G Suite' and 'All users in this account'. The main content area shows a table of service statuses for all organizational units. The 'Gmail' row is highlighted with a red box.

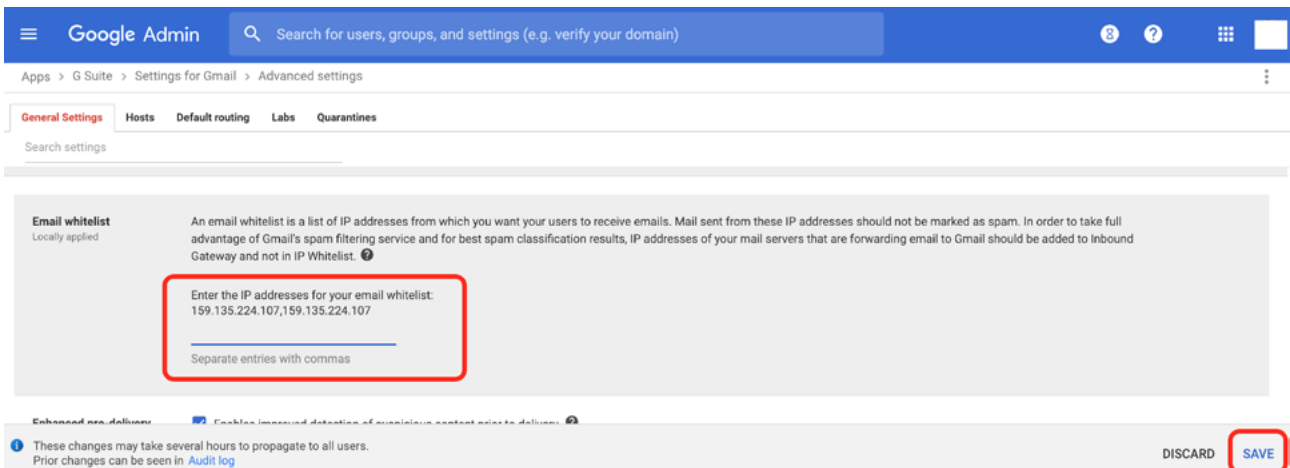
Showing status for apps in all organizational units		ADD SERVICE
<input type="checkbox"/> Services ↑		Service Status
<input type="checkbox"/>	Calendar	ON for everyone
<input type="checkbox"/>	Drive and Docs	ON for everyone
<input type="checkbox"/>	Gmail	ON for everyone
<input type="checkbox"/>	Google+	ON for everyone
<input type="checkbox"/>	Google Hangouts	ON for everyone
<input type="checkbox"/>	Hangouts Chat	ON for everyone

Select Advanced Settings



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

- 159.135.224.107
- 104.130.122.237

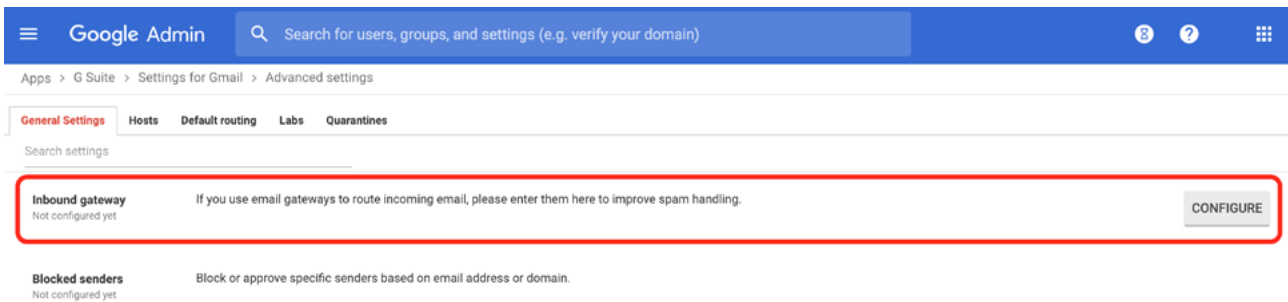


Part 2: Add IP addresses as Inbound Gateways

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 > G Suite > 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**

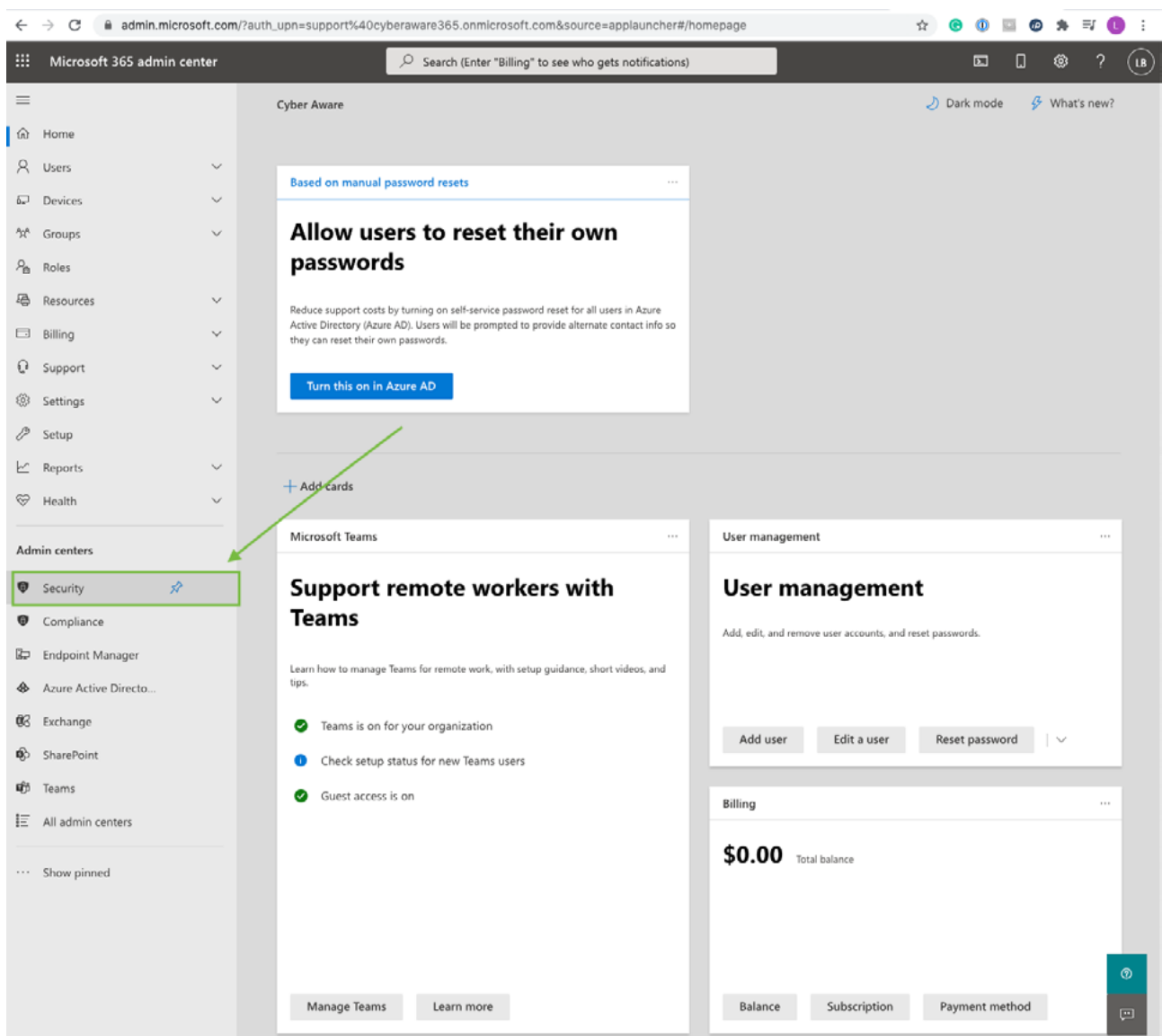
5. Select the **Disable Gmail spam evaluation on mail from this gateway; only useheader value**

6. Click the **ADD SETTING** button

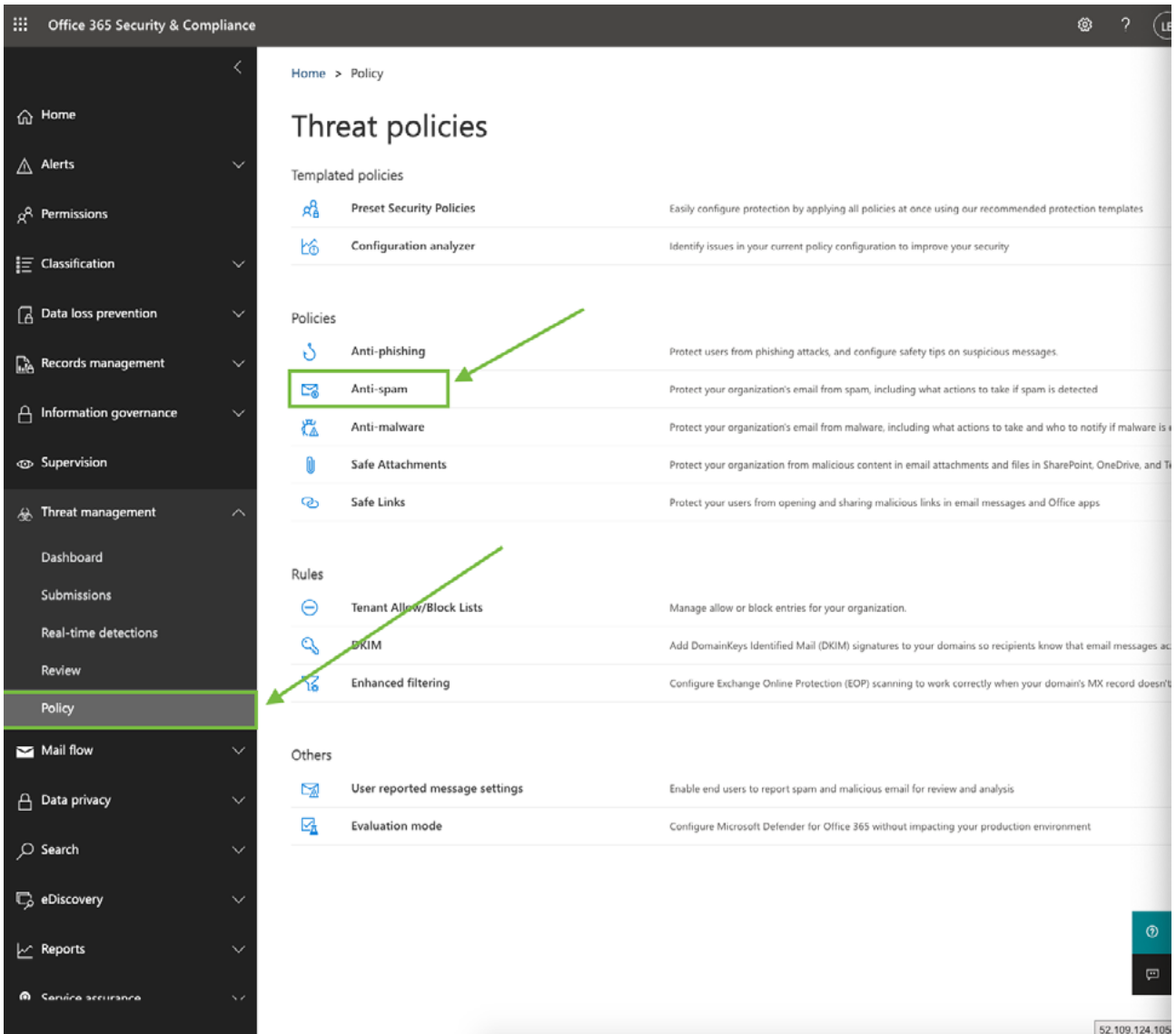
SECTION 2:

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

The screenshot displays the Office 365 Security & Compliance console. On the left is a navigation pane with categories like Home, Alerts, Permissions, Classification, Data loss prevention, Records management, Information governance, Supervision, Threat management, Policy, Mail flow, Data privacy, Search, eDiscovery, Reports, and Service assurance. The main area shows 'Anti-spam policies' with a table of policies:

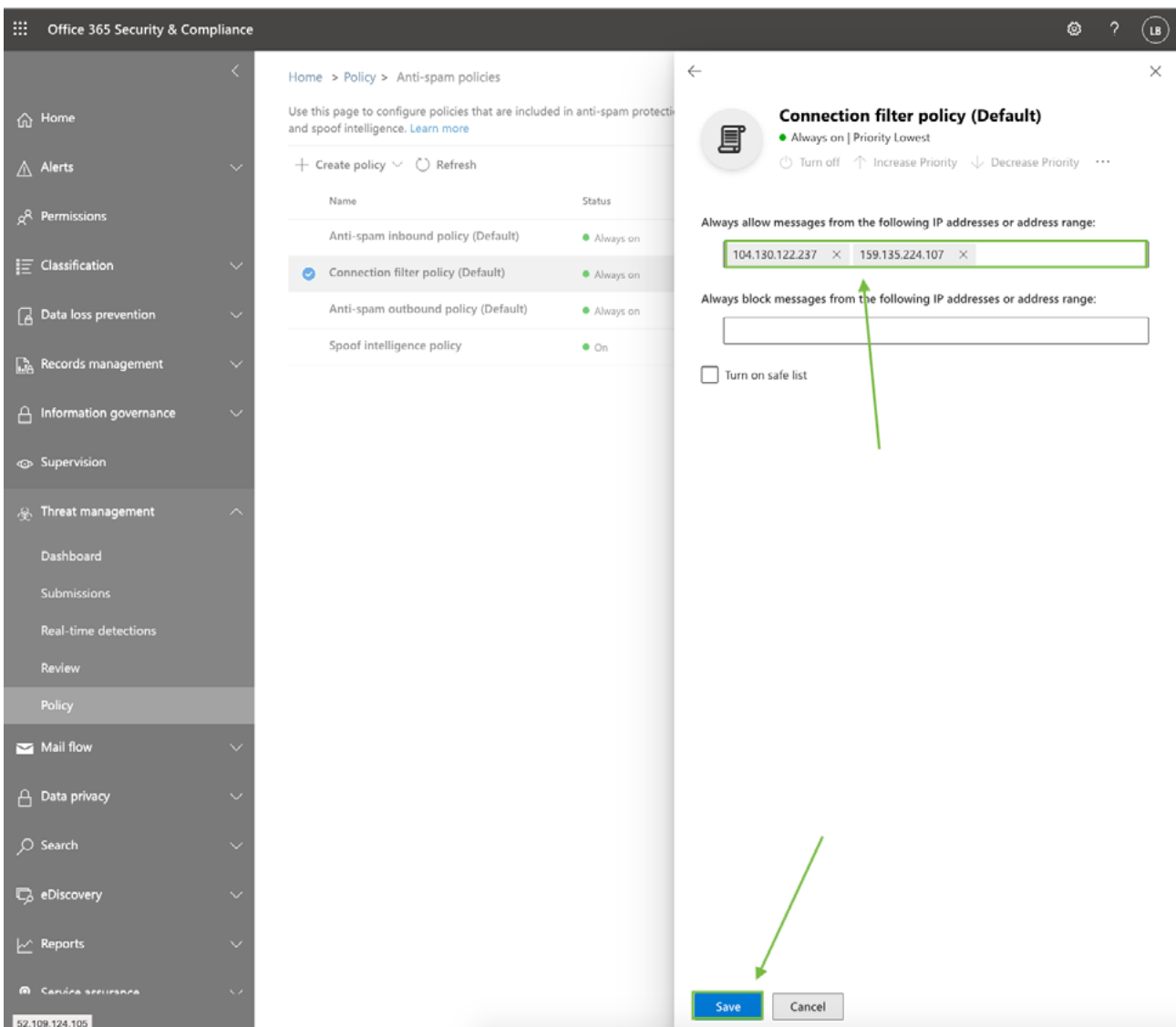
Name	Status
Anti-spam inbound policy (Default)	Always on
Connection filter policy (Default)	Always on
Anti-spam outbound policy (Default)	Always on
Spoof intelligence policy	On

The 'Connection filter policy (Default)' row is highlighted with a green box. A green arrow points from the text 'Double Click Here' to this row. Another green arrow points from the same text to the 'Edit connection filter policy' button in the right-hand configuration pane. The configuration pane shows the policy is 'Always on | Priority Lowest' and includes sections for 'Description', 'Connection filtering', 'IP Allow list', 'IP Block list', and 'Safe list'. A 'Close' button is at the bottom right of the configuration pane.

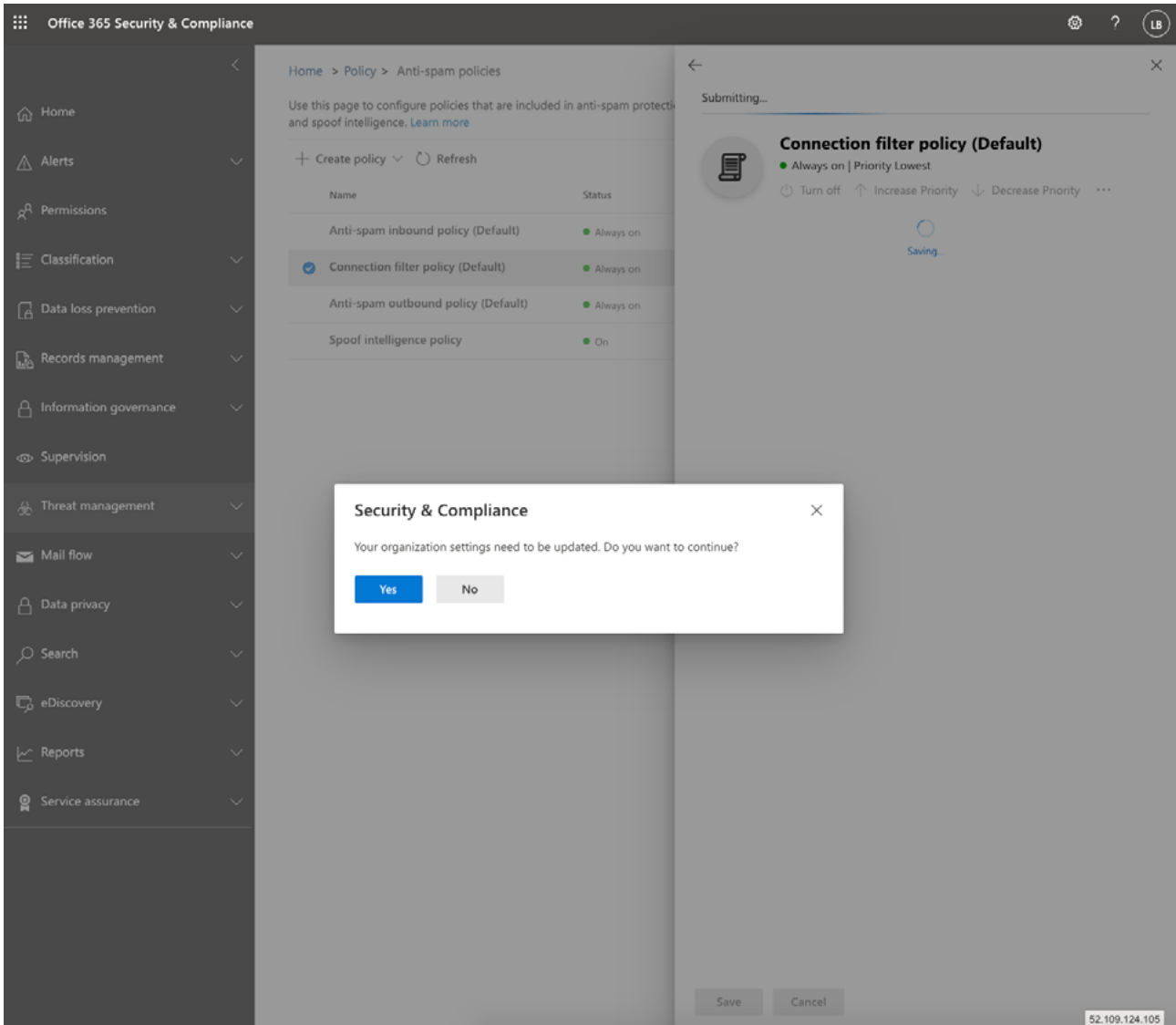
4. Enter the following IP Addresses then click **Save**:

a. 104.130.122.237

b. 159.135.224.107

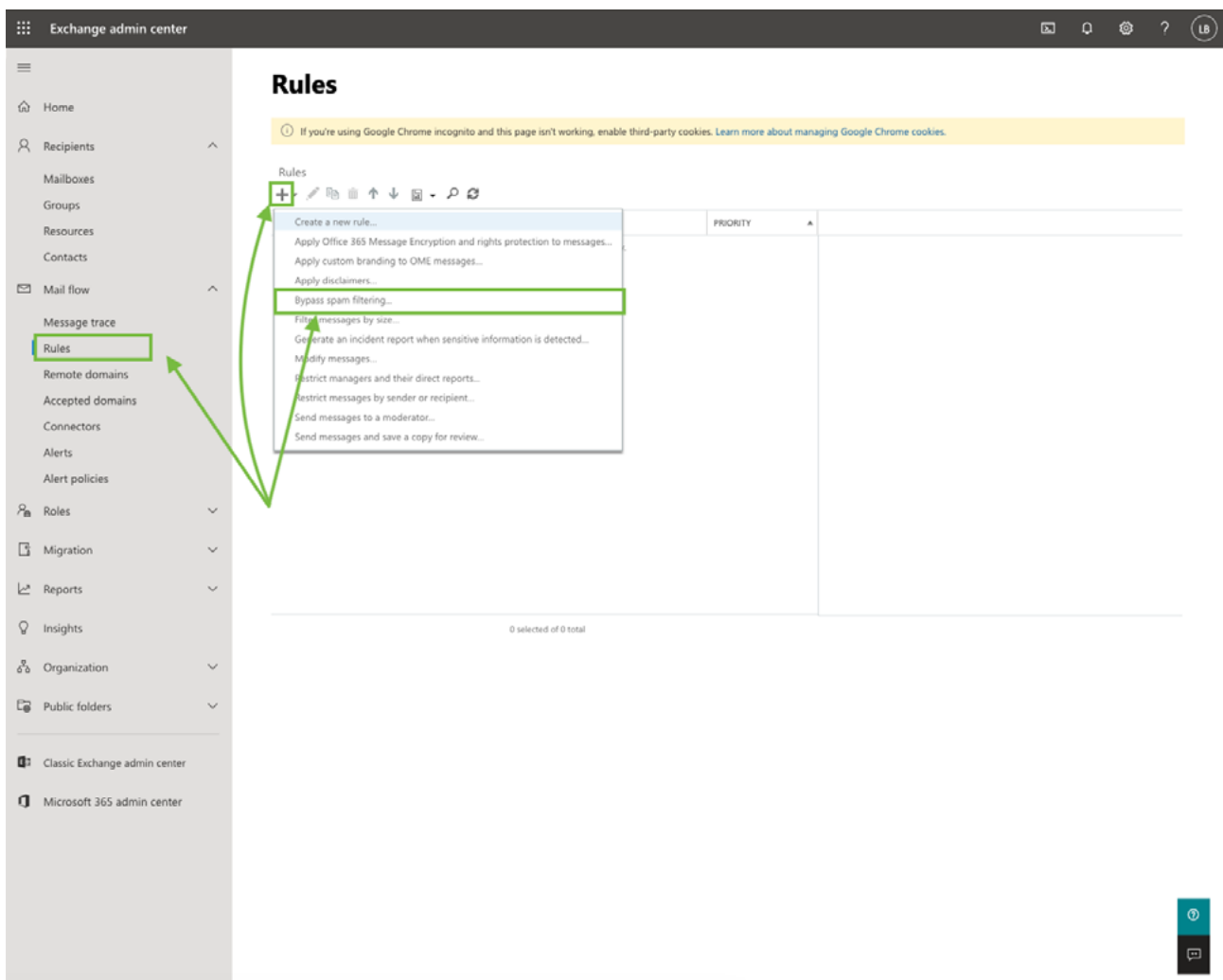


5. If the following prompt pops up, click **Yes**



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

1 Awareness Campaign Spam Filter by IP Address

2 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]

3 IP address is in any of these ranges or exactly matches

Save Cancel

4. Click “Enter IPv4 or IPv6 addresses...” and enter

- a. 104.130.122.237
- b. 159.135.224.107

1 Enter IPv4 or IPv6 addresses...

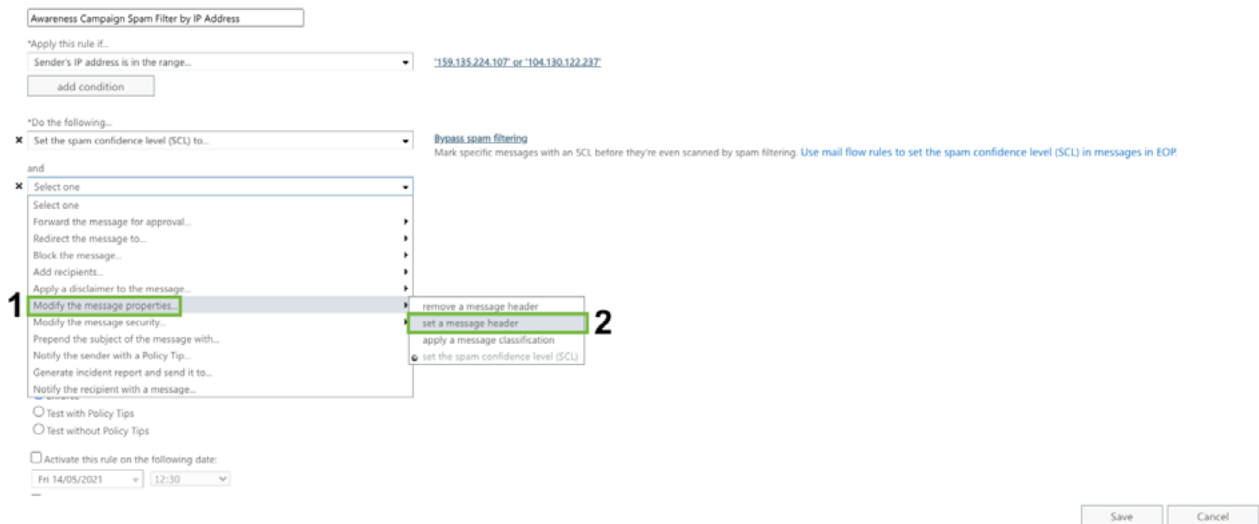
2 specify IP address ranges

3 OK

Save Cancel

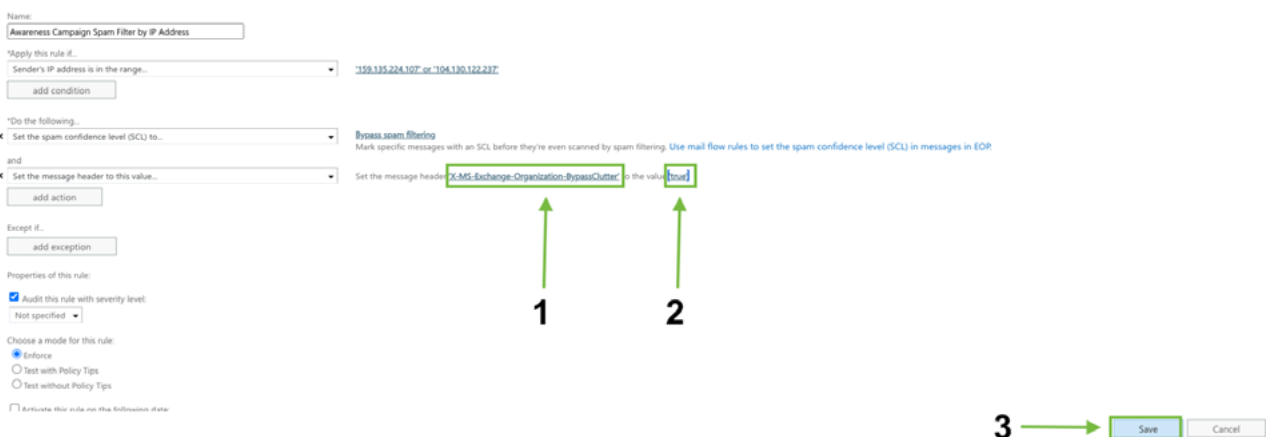
5. Add a message header

- a. Click **Add Action**
- b. Click **'Modify the message properties'** > **'Set a Message Header'**



6. Modify the message header and value:

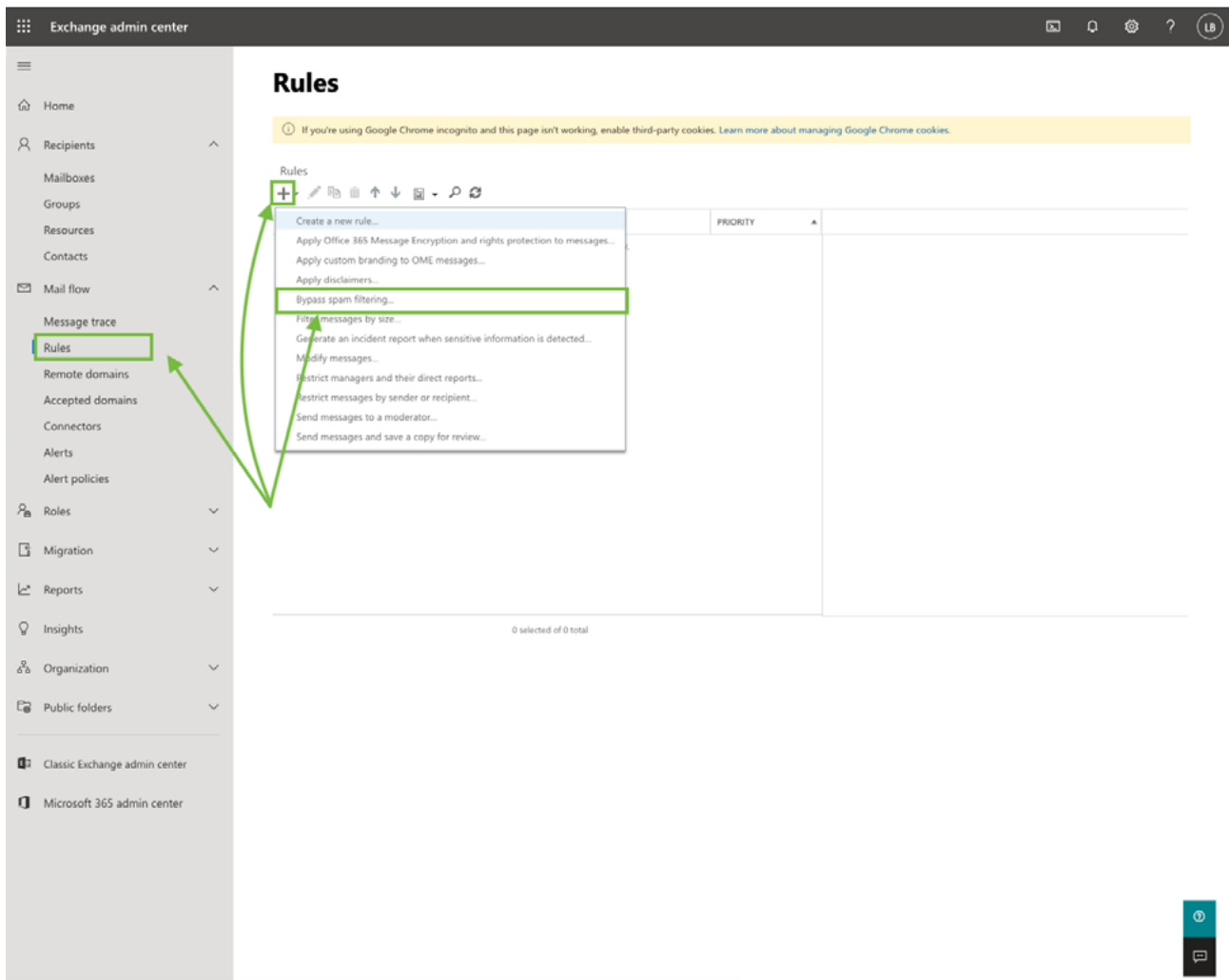
- a. Click on Set a message header **"Enter text..."** and add the following (case sensitive!):
 - a. X-MS-Exchange-Organization-BypassClutter
- b. Click on ... to the value **"Enter text..."** and add (case sensitive!):
 - a. true
- c. Click **Save**



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*

1 **Name:** Focused Inbox Whitelisting

2 **Apply this rule if...**
 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]
 Properties of this rule:
 Audit this rule with severity level:
 Not specified

3 **IP address is in any of these ranges or exactly matches**

Save Cancel

3. Click “Enter IPv4 or IPv6 addresses...” and enter

a. 104.130.122.237

b. 159.135.224.107

Awareness Campaign Spam Filter by IP Address

Name: Awareness Campaign Spam Filter by IP Address

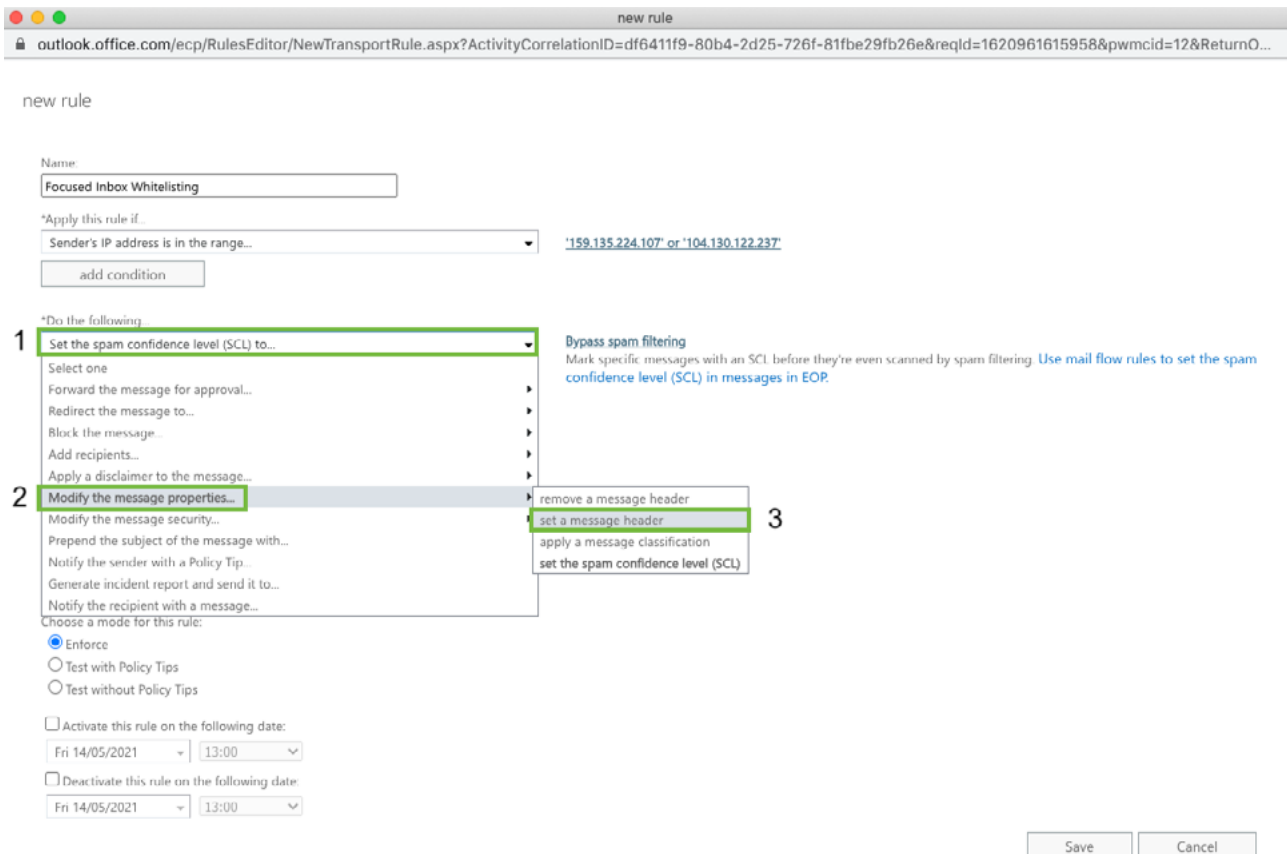
1 **Apply this rule if...**
 Sender's IP address is in the range...
 add condition
 Enter IPv4 or IPv6 addresses...

2 **specify IP address ranges**
 Enter an IPv4 or IPv6 address, or range

3 **OK**

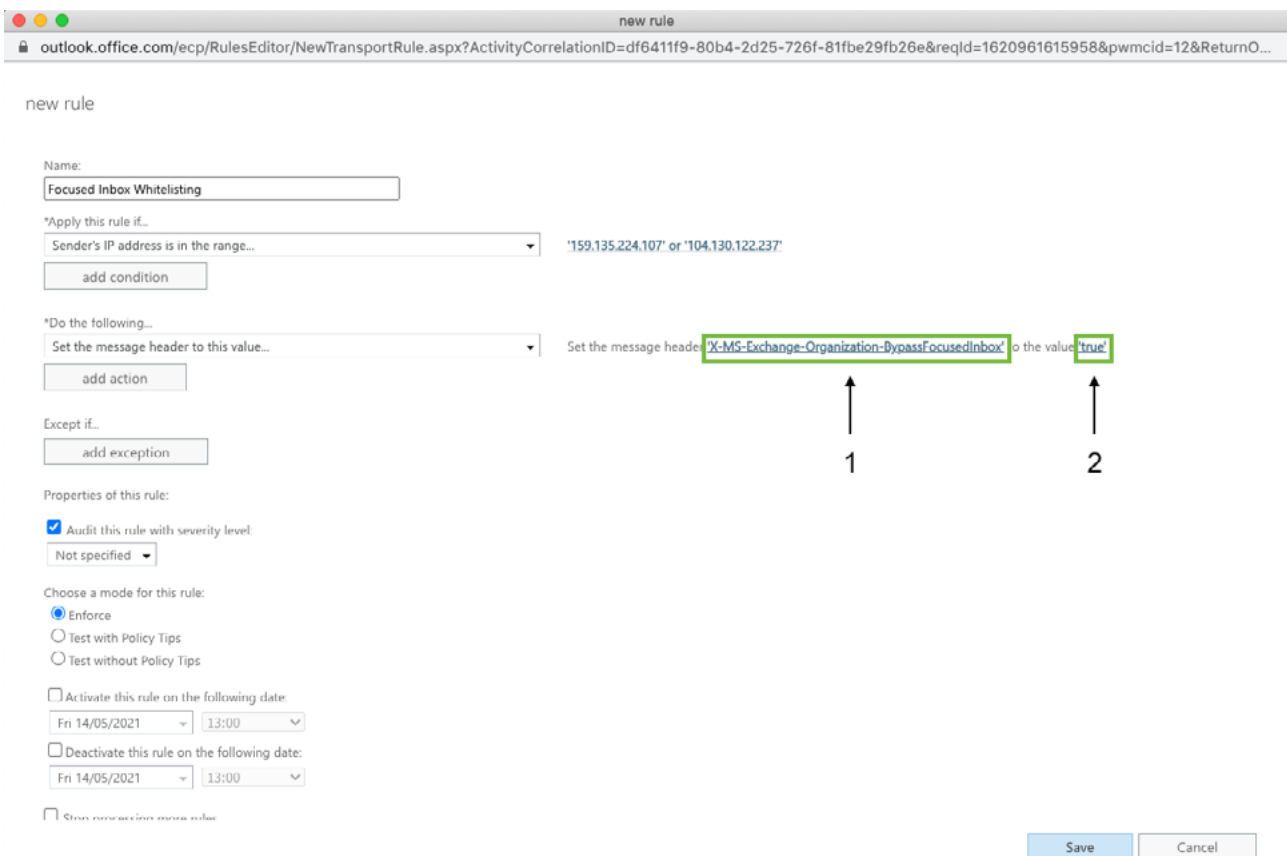
Save Cancel

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:

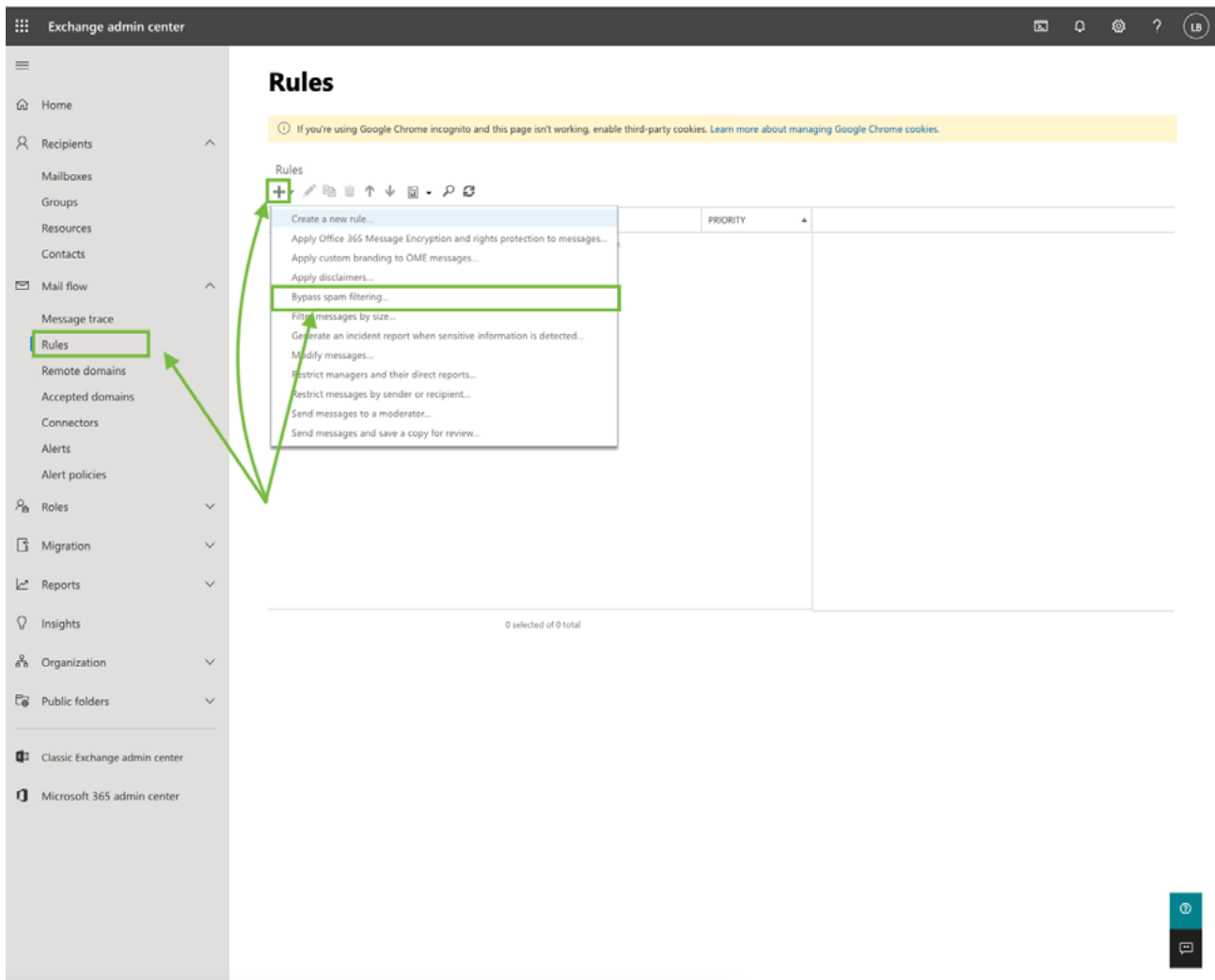
- a. Click on Set a message header “**Enter text...**” and add the following (case sensitive!):
 - a. X-MS-Exchange-Organization-BypassFocusedInbox
- b. Click on ... to the value “**Enter text...**” and add (case sensitive!):
 - a. true



Add Mail Flow rule to skip junk filtering

1. Go to Mail Flow > Rules

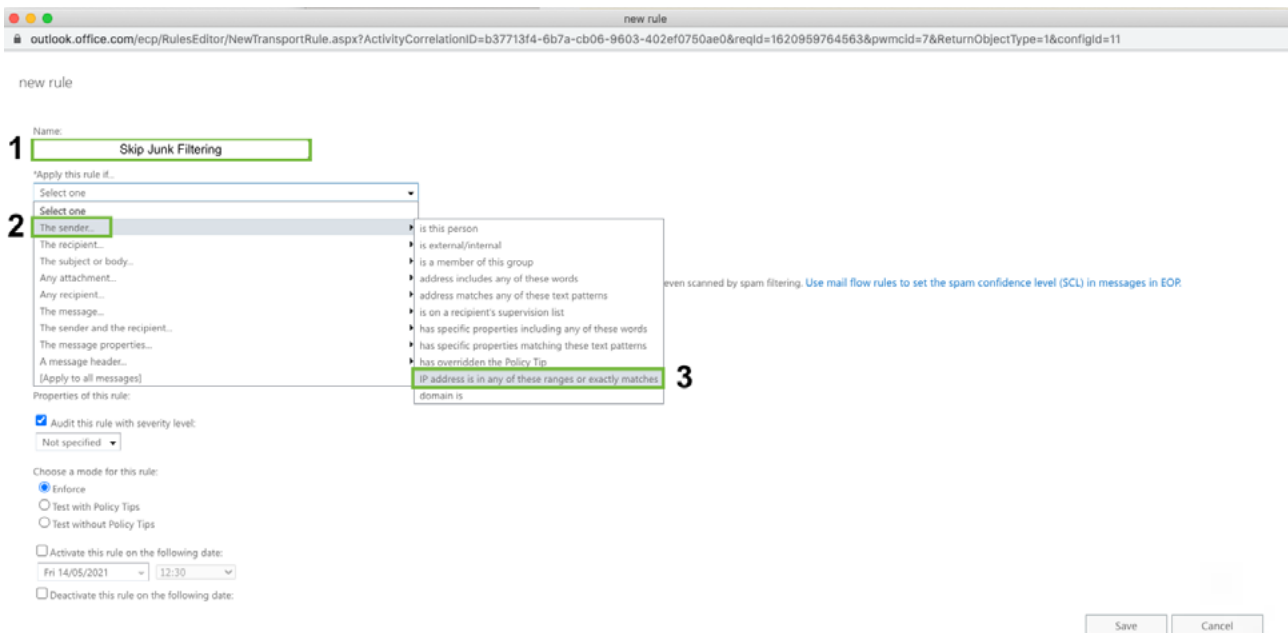
a. Create a Bypass Spam Filtering Rule



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

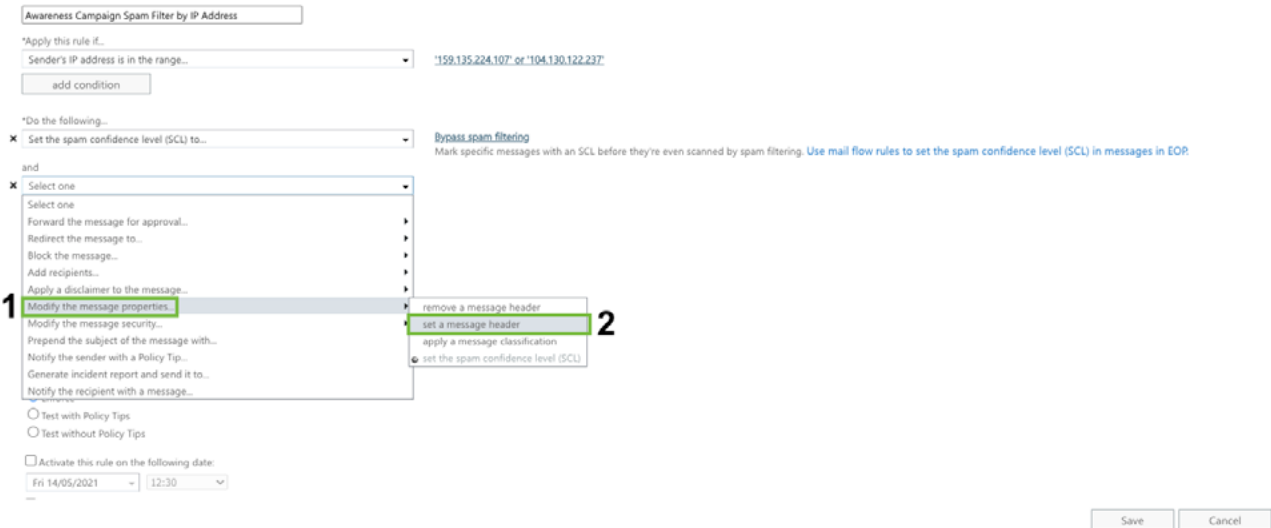
a. 104.130.122.237

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:

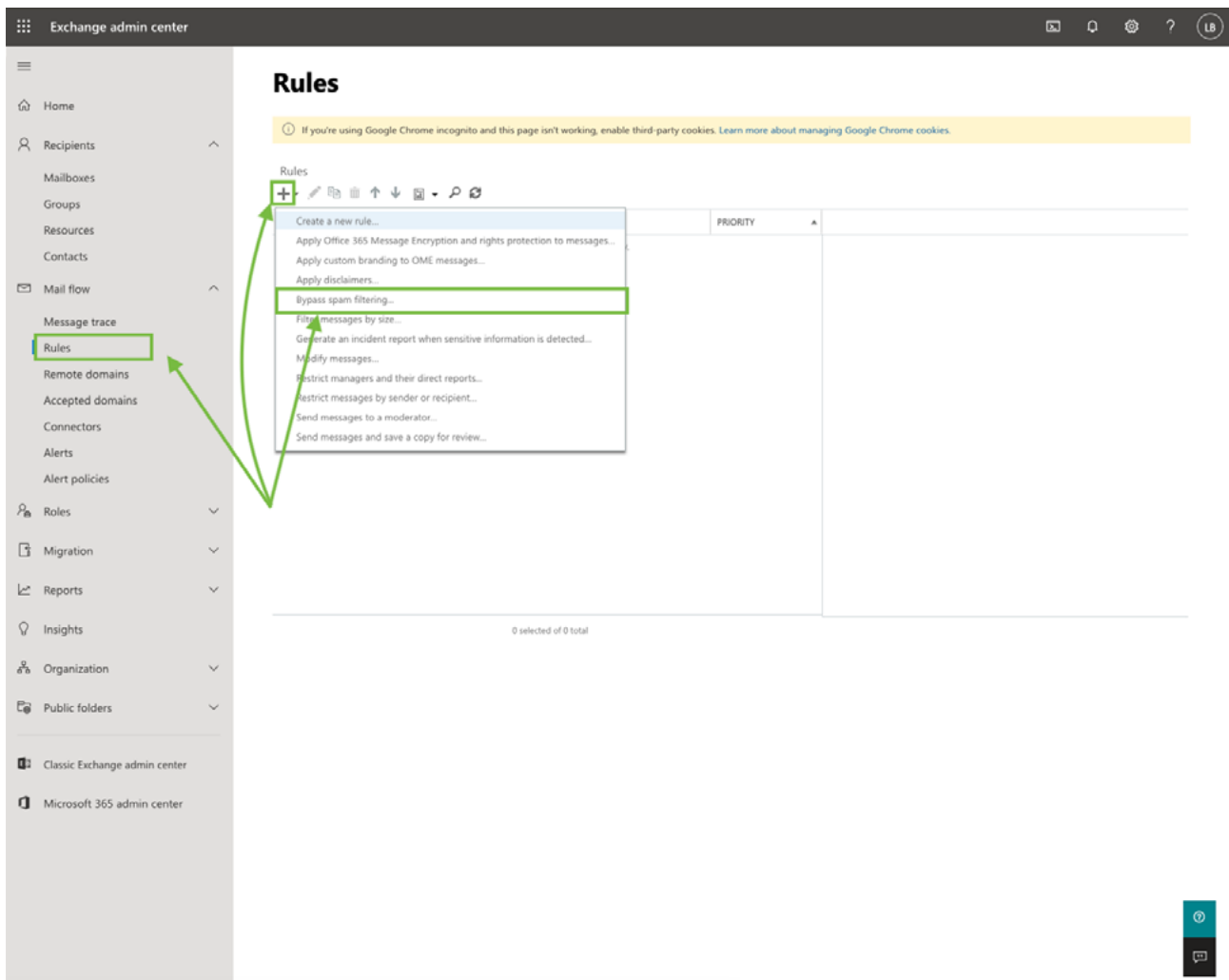
- a. Click on Set a message header **“Enter text...”** and add the following (case sensitive!):
 - a. X-Forefront-Antispam-Report
- b. Click on ... to the value **“Enter text...”** and add (case sensitive!):
 - a. SFV:SKJ;



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*

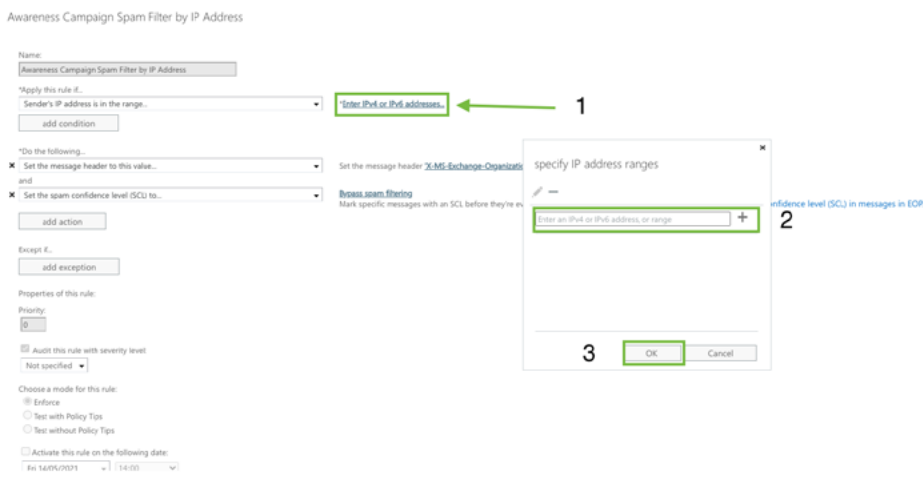
b. **Apply this rule if:** *The sender IP address is any of these ranges or exactly matches*



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:

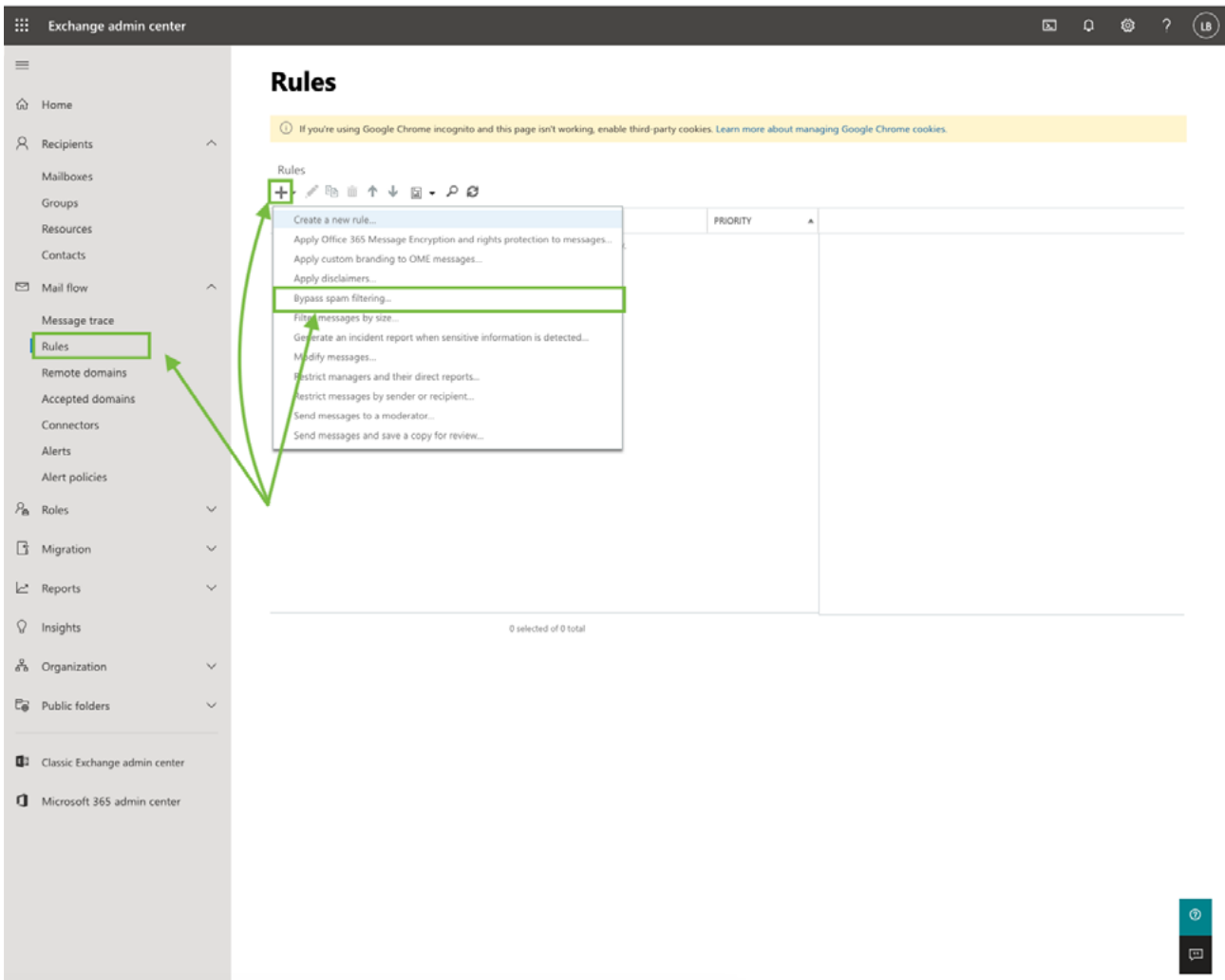
- a. Click on Set a message header **“Enter text...”** and add the following (case sensitive!):
 - a. X-MS-Exchange-Organization-SkipSafeLinksProcessing
- b. Click on ... to the value **“Enter text...”** and add (case sensitive!):
 - a. 1

new rule

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*

new rule

3. Click “Enter IPv4 or IPv6 addresses...” and enter

a. 104.130.122.237

b. 159.135.224.107

Awareness Campaign Spam Filter by IP Address

4. Replace the Bypass Spam Filtering Rule:

- a. Click ***Do the Following....**
- b. Modify the **message properties** > set a message header

new rule

Awareness Campaign Spam Filter by IP Address

*Apply this rule if...

Sender's IP address is in the range... '159.135.224.107' or '104.130.122.237'

add condition

*Do the following...

Set the spam confidence level (SCL) to...

Bypass spam filtering
Mark specific messages with an SCL before they're even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

and

Select one

- Select one
- Forward the message for approval...
- Redirect the message to...
- Block the message...
- Add recipients...
- Apply a disclaimer to the message...
- 1 Modify the message properties...**
- Modify the message security...
- Prepend the subject of the message with...
- Notify the sender with a Policy Tip...
- Generate incident report and send it to...
- Notify the recipient with a message...

- remove a message header
- 2 set a message header**
- apply a message classification
- set the spam confidence level (SCL)

Test with Policy Tips

Test without Policy Tips

Activate this rule on the following date:

Fri 14/05/2021 12:30

Save Cancel

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

Bypass ATP Attachments

Name:

Bypass ATP Attachments

*Apply this rule if...

Sender's IP address is in the range... '104.130.122.237' or '159.135.224.107'

add condition

*Do the following...

Set the message header to this value...

Set the message header 'X-MS-Exchange-Organization-SkipSafeAttachmentProcessing' to the value '1'

add action

Except if...

add exception

Properties of this rule

Priority:

4

Audit this rule with severity level.

Not specified

Save Cancel



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