Business Australia Cyber

Phishing Whitelisting Guide

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

104.130.122.237

159.135.224.107

Business Australia 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:

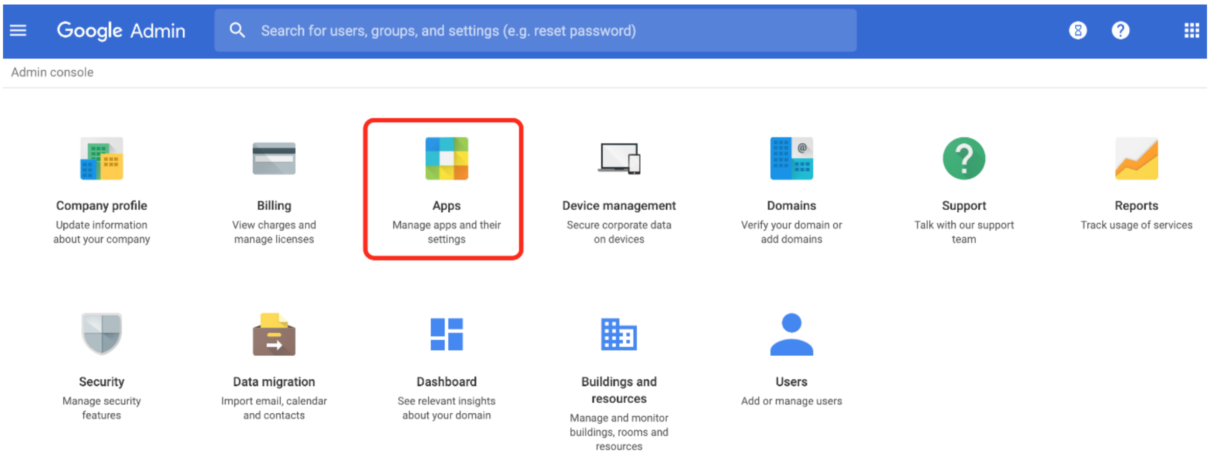
Gmail/G Suite/Google Apps

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.

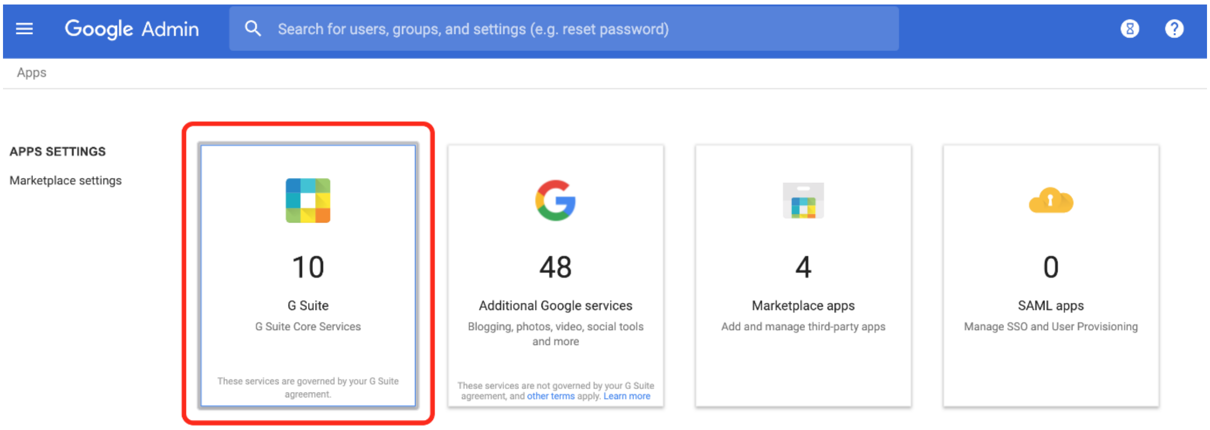
We recommend setting up a test phishing campaign to yourself or a low volume sending group after you follow the below steps to ensure your whitelisting was successful. The setting may take up to an hour to propagate to all users.

Part 1: Add Sending IP addresses to email whitelist

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


Google Admin
Search for users, groups, and settings (e.g. reset password)
Admin console
Company profile
Update information about your company
Billing
View charges and manage licenses
Apps
Manage apps and their settings
Device management
Secure corporate data on devices
Domains
Verify your domain or add domains
Support
Talk with our support team
Reports
Track usage of services
Security
Manage security features
Data migration
Import email, calendar and contacts
Dashboard
See relevant insights about your domain
Buildings and resources
Manage and monitor buildings, rooms and resources
Users
Add or manage users

Select **G Suite**.


Google Admin
Search for users, groups, and settings (e.g. reset password)
Apps
APPS SETTINGS
Marketplace settings

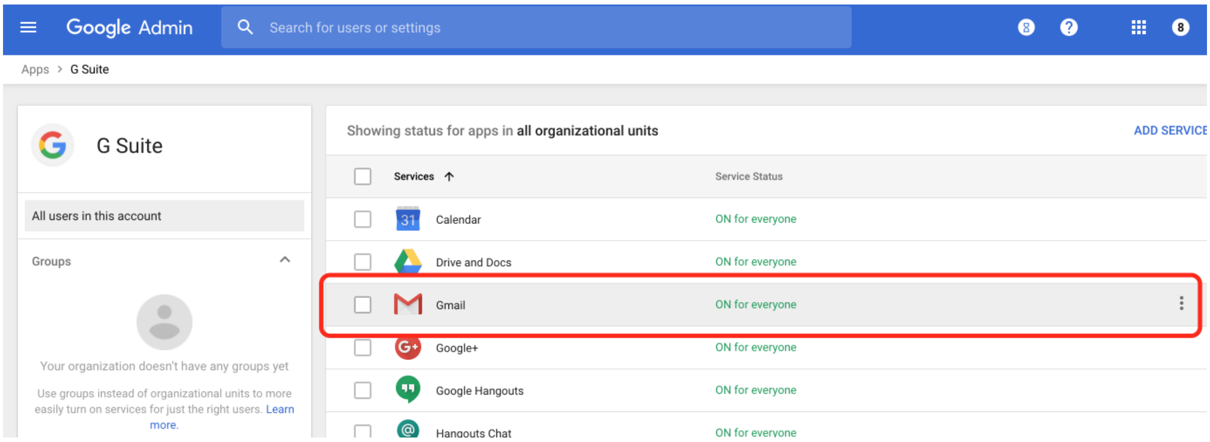
10
G Suite
G Suite Core Services
These services are governed by your G Suite agreement.

48
Additional Google services
Blogging, photos, video, social tools and more
These services are not governed by your G Suite agreement, and other terms apply. Learn more

4
Marketplace apps
Add and manage third-party apps

0
SAML apps
Manage SSO and User Provisioning

Select **Gmail**.



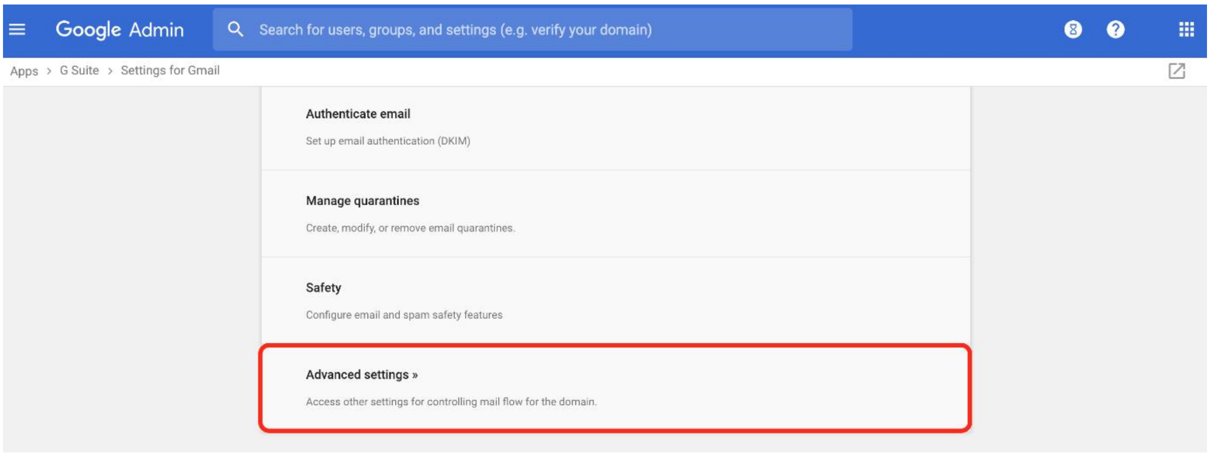
Your organization doesn't have any groups yet

Use groups instead of organizational units to more easily turn on services for just the right users. Learn more.

Showing status for apps in **all organizational units**

Services	Service Status
Calendar	ON for everyone
Drive and Docs	ON for everyone
Gmail	ON for everyone
Google+	ON for everyone
Google Hangouts	ON for everyone
Hangouts Chat	ON for everyone

Select **Advanced Settings**.


Google Admin
Search for users, groups, and settings (e.g. verify your domain)
Apps > G Suite > Settings for Gmail

Authenticate email
Set up email authentication (DKIM)

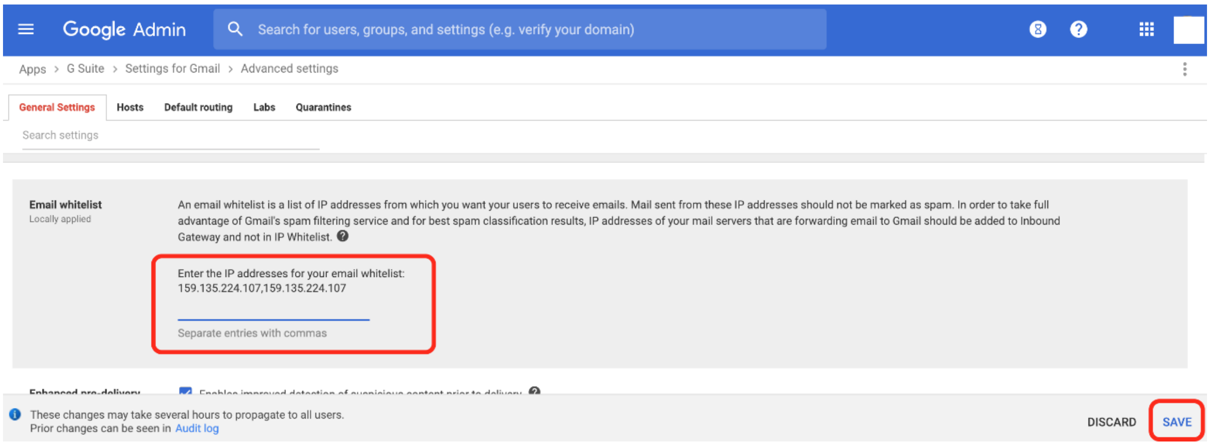
Manage quarantines
Create, modify, or remove email quarantines.

Safety
Configure email and spam safety features

Advanced settings »
Access other settings for controlling mail flow for the domain.

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

- 159.135.224.107
- 104.130.122.237


Google Admin
Search for users, groups, and settings (e.g. verify your domain)
Apps > G Suite > Settings for Gmail > Advanced settings
General Settings
Hosts
Default routing
Labs
Quarantines
Search settings
DISCARD
SAVE

Email whitelist
Locally applied

An email whitelist is a list of IP addresses from which you want your users to receive emails. Mail sent from these IP addresses should not be marked as spam. In order to take full advantage of Gmail's spam filtering service and for best spam classification results, IP addresses of your mail servers that are forwarding email to Gmail should be added to Inbound Gateway and not in IP Whitelist.

Enter the IP addresses for your email whitelist:
159.135.224.107,159.135.224.107

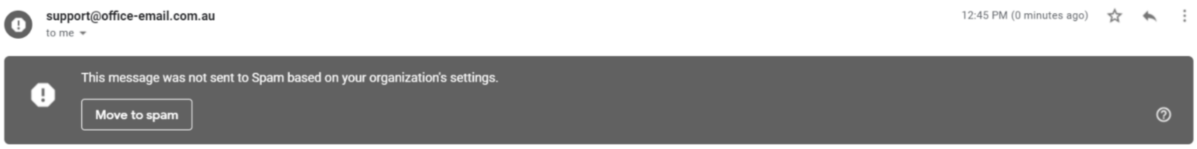
Separate entries with commas

Enhanced pre-delivery ☑ Enables improved detection of suspicious content prior to delivery

These changes may take several hours to propagate to all users.
Prior changes can be seen in Audit log

Part 2: Add IP addresses as Inbound Gateways

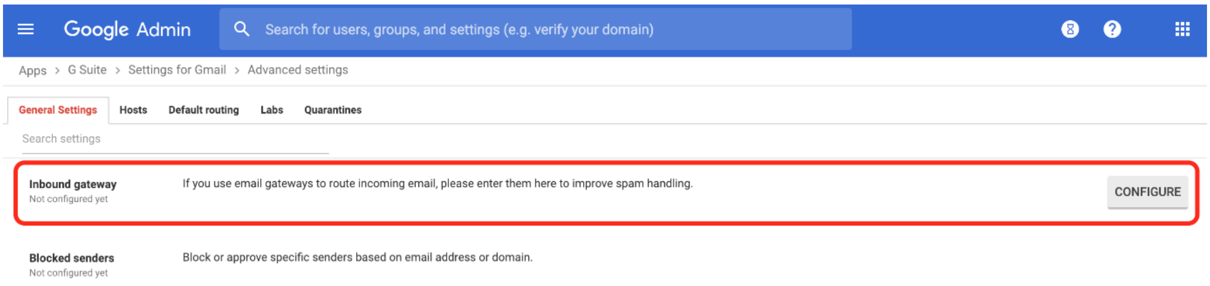
This method of whitelisting is to prevent the following Google banners from appearing in your user's inbox:



support@office-email.com.au
to me
12:45 PM (0 minutes ago)

This message was not sent to Spam based on your organization's settings.

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. Hover over the setting and click the **Edit** button. This will open the **Inbound gateway** screen.

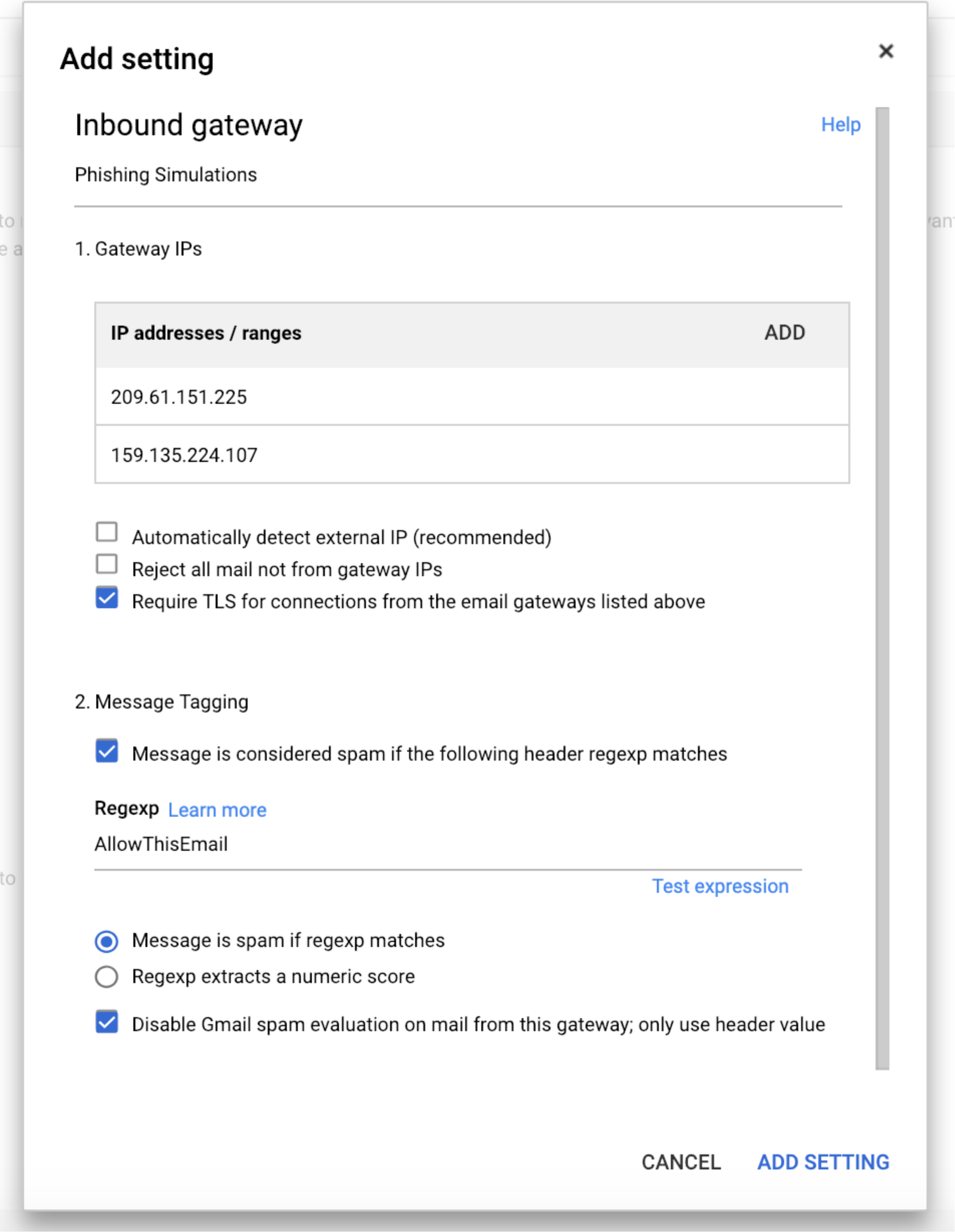


Google Admin
Search for users, groups, and settings (e.g. verify your domain)
Apps > G Suite > Settings for Gmail > Advanced settings
General Settings
Hosts
Default routing
Labs
Quarantines
Search settings
CONFIGURE

Inbound gateway
Not configured yet
If you use email gateways to route incoming email, please enter them here to improve spam handling.

Blocked senders
Not configured yet
Block or approve specific senders based on email address or domain.

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



Add setting

Inbound gateway

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

AllowThisEmail

● Message is spam if regexp matches

○ Regexp extracts a numeric score

☑ Disable Gmail spam evaluation on mail from this gateway; only use header value

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**

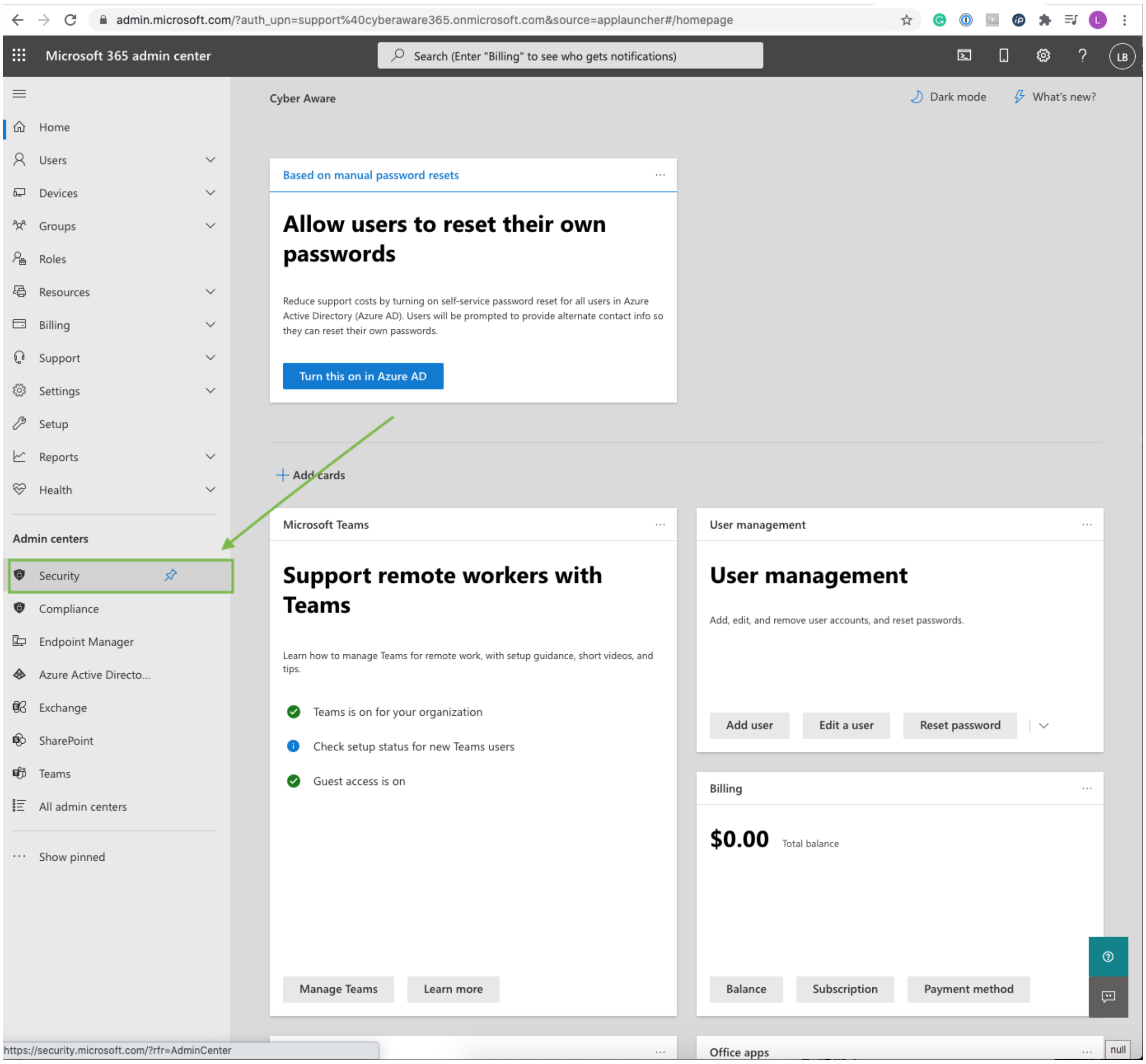
   Enter text "**AllowThisEmail**" for the **Spam Header Tag**.

5. Select the **Disable Gmail spam evaluation on mail from this gateway; only use header value**.
6. Click the **ADD SETTING** button.

SECTION 2:

Office 365 Instructions

1. Log in to Office 365 and go to Security



Allow users to reset their own passwords

Reduce support costs by turning on self-service password reset for all users in Azure Active Directory (Azure AD). Users will be prompted to provide alternate contact info so they can reset their own passwords.

Support remote workers with Teams

Learn how to manage Teams for remote work, with setup guidance, short videos, and tips.

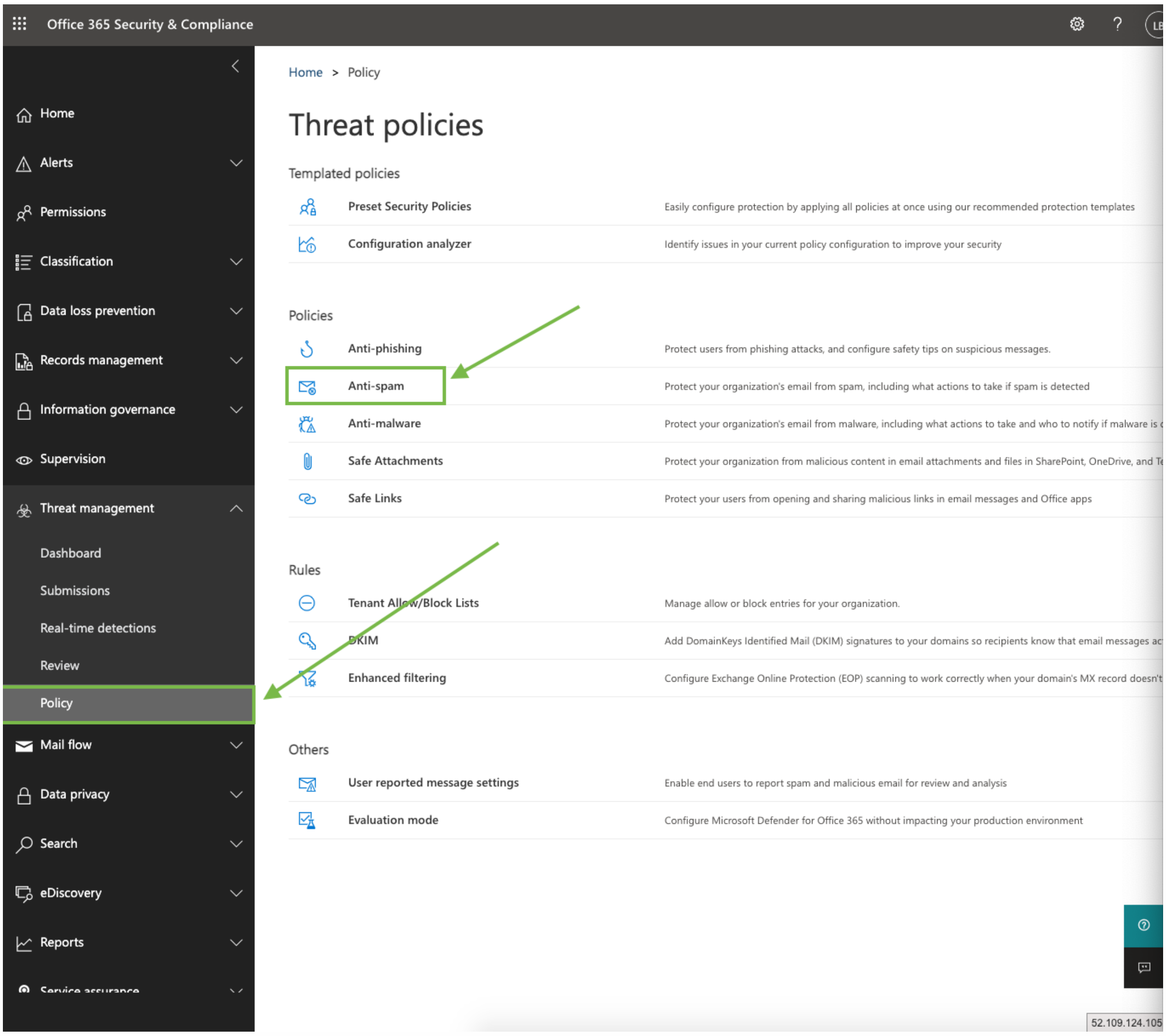
- Teams is on for your organization
- Check setup status for new Teams users
- Guest access is on

User management

Add, edit, and remove user accounts, and reset passwords.

$0.00 Total balance

2. Go to Policy > Anti-spam



Home > Policy

Threat policies

Templated policies

Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
Configuration analyzer	Identify issues in your current policy configuration to improve your security

Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is c
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Te
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

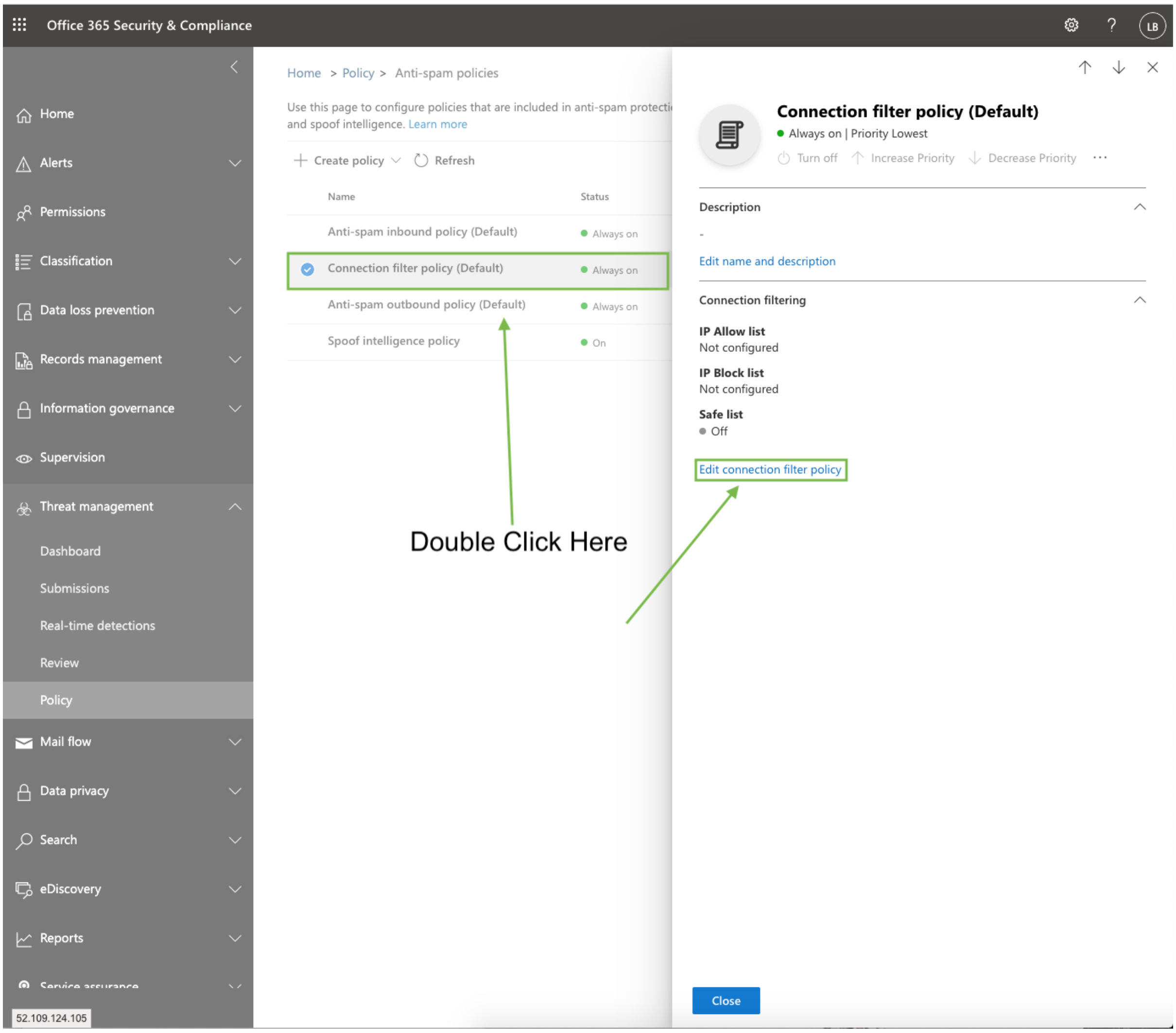
Rules

Tenant Allow/Block Lists	Manage allow or block entries for your organization.
DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages ac
Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't

Others

User reported message settings	Enable end users to report spam and malicious email for review and analysis
Evaluation mode	Configure Microsoft Defender for Office 365 without impacting your production environment

3. Double click ‘Connection Filter Policy’ > Click Edit Connection Filter Policy



Use this page to configure policies that are included in anti-spam protecti and spoof intelligence. Learn more

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

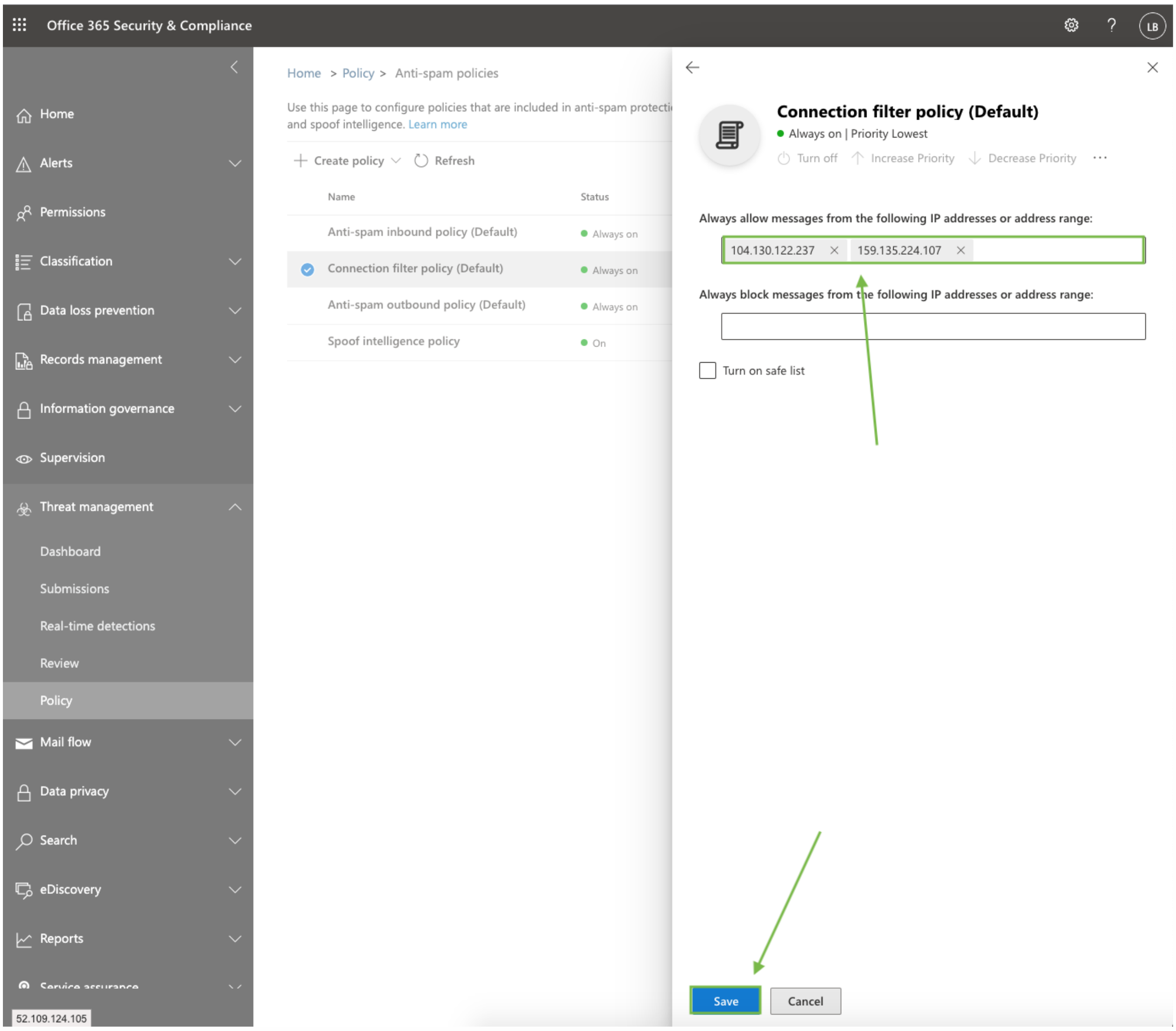
Connection filter policy (Default)
● Always on | Priority Lowest
Turn off   Increase Priority   Decrease Priority

Description
-
Edit name and description

Connection filtering
IP Allow list
Not configured
IP Block list
Not configured
Safe list
● Off

Edit connection filter policy

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



Use this page to configure policies that are included in anti-spam protecti and spoof intelligence. Learn more

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

Connection filter policy (Default)

Always on | Priority Lowest

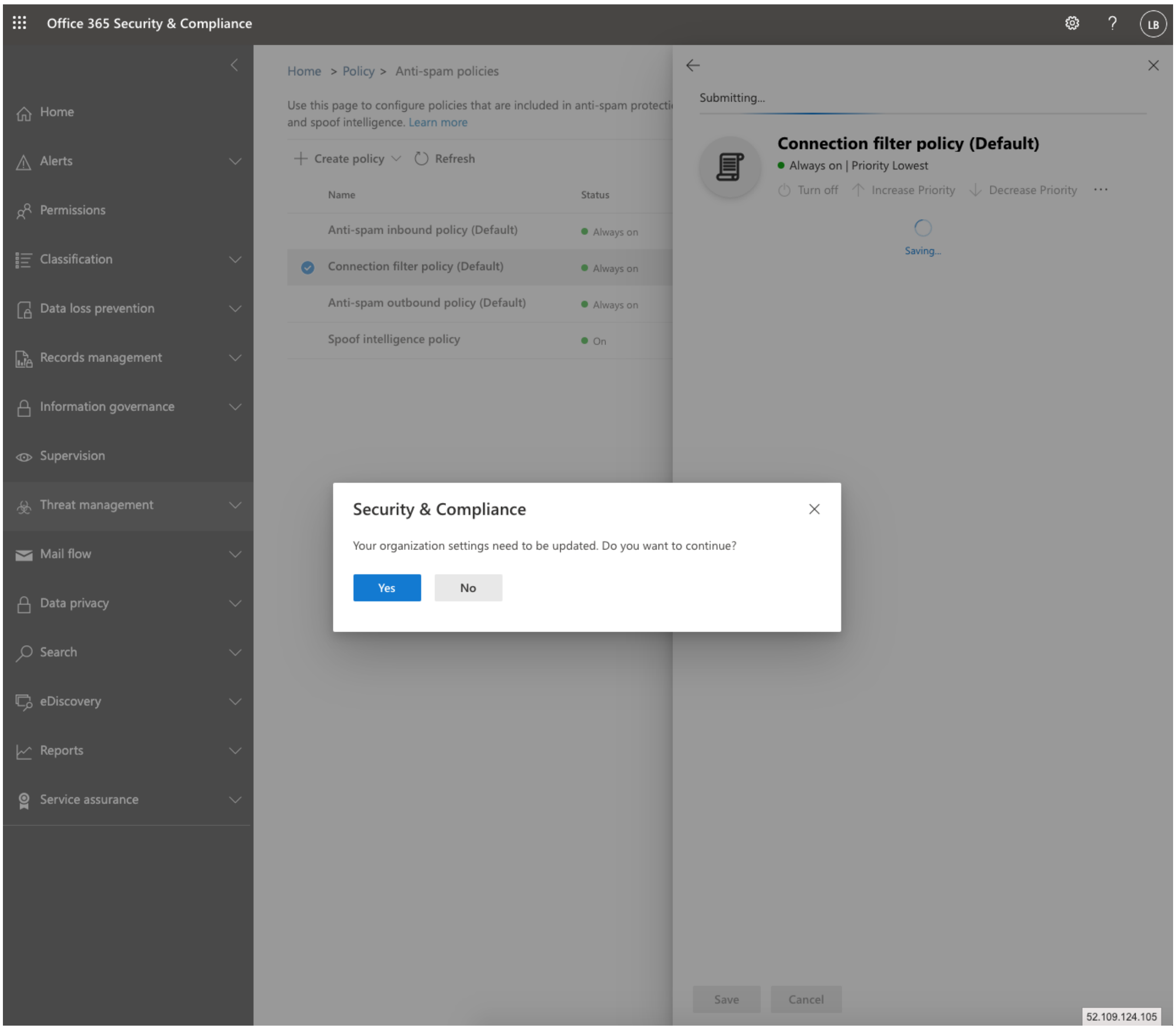
Always allow messages from the following IP addresses or address range:

104.130.122.237 159.135.224.107

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

□ Turn on safe list

5. If the following prompt pops up, click Yes



Use this page to configure policies that are included in anti-spam protecti and spoof intelligence. Learn more

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

Connection filter policy (Default)
Always on | Priority Lowest

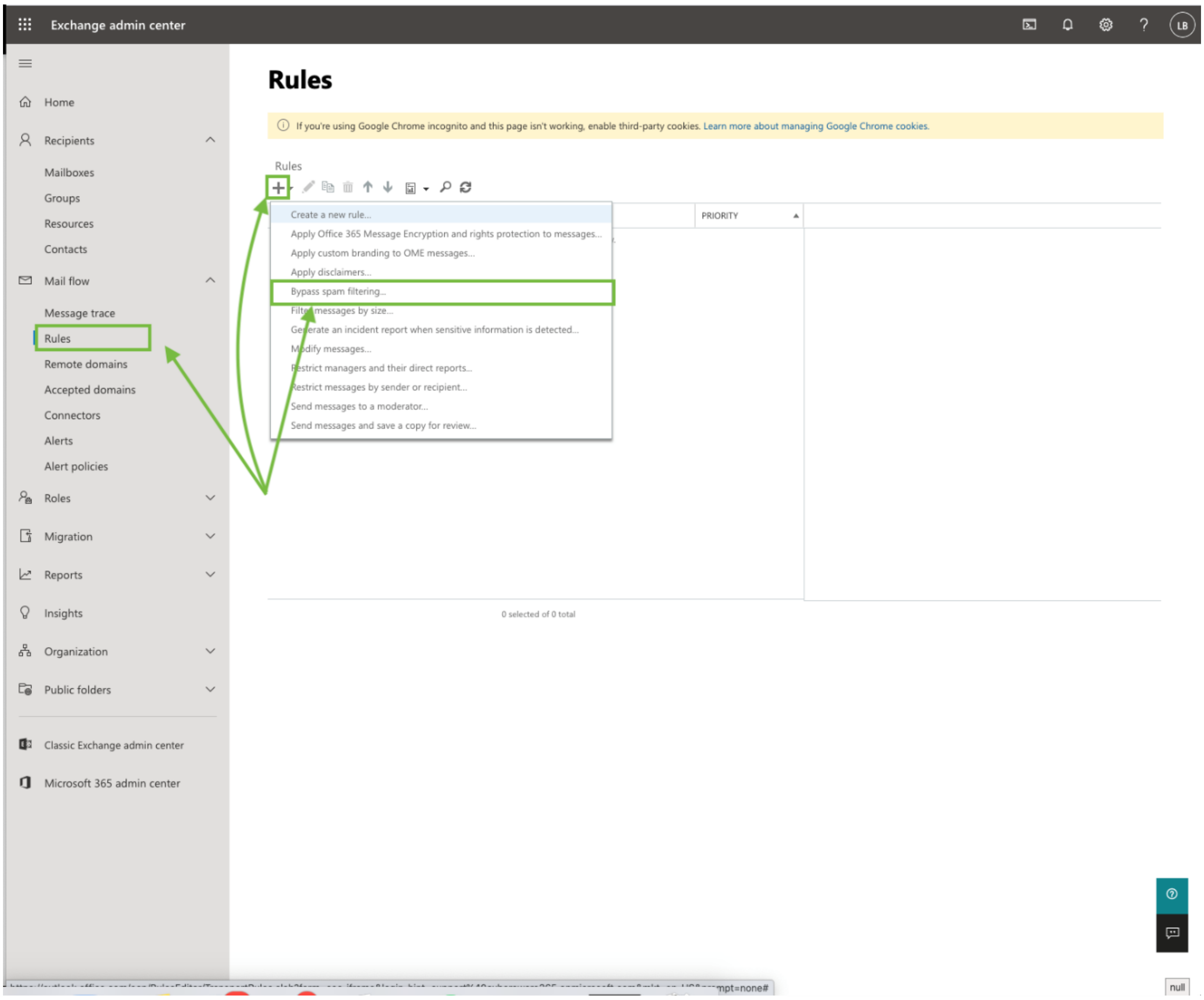
Security & Compliance

Your organization settings need to be updated. Do you want to continue?

Yes No

Add Mail Flow rules to bypass spam filtering and clutter

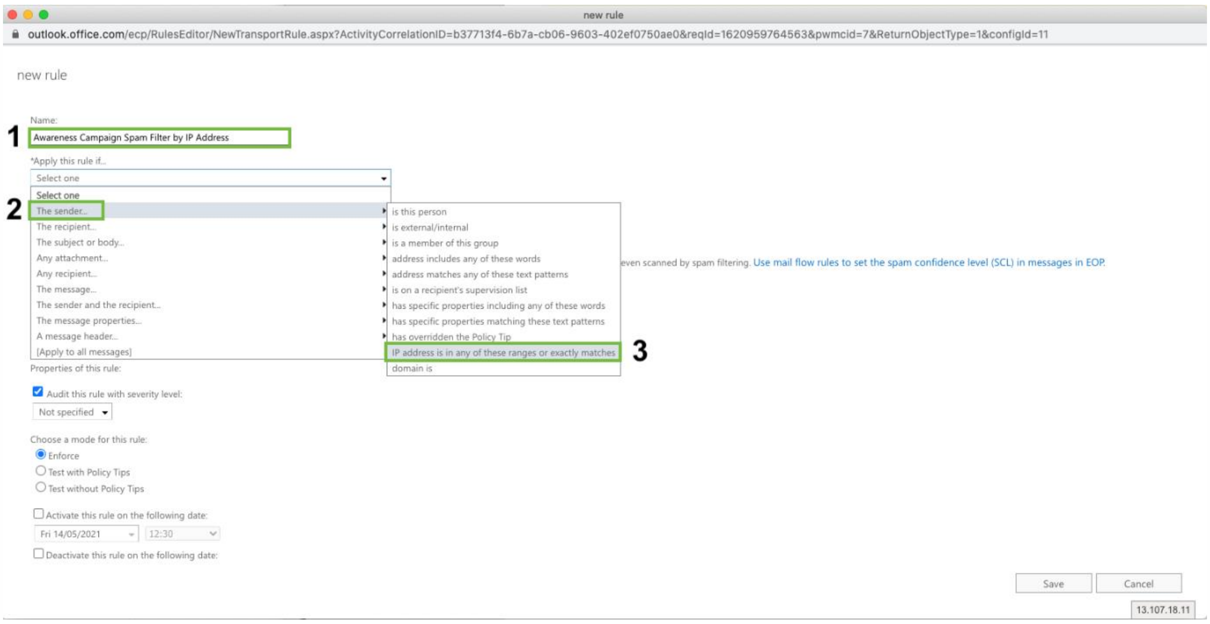
1. Go to your Exchange admin centre.
   a. This can be found via the following URL: **https://admin.exchange.microsoft.com**
2. Go to Mail Flow > Rules
   a. Create a Bypass Spam Filtering Rule


Exchange admin center
Home
Recipients
Mailboxes
Groups
Resources
Contacts
Mail flow
Message trace
Rules
Remote domains
Accepted domains
Connectors
Alerts
Alert policies
Roles
Migration
Reports
Insights
Organization
Public folders
Classic Exchange admin center
Microsoft 365 admin center
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...
PRIORITY
0 selected of 0 total
null

If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. Learn more about managing Google Chrome cookies.

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*



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

Name: Awareness Campaign Spam Filter by IP Address

*Apply this rule if... Select one

Audit this rule with severity level: Not specified

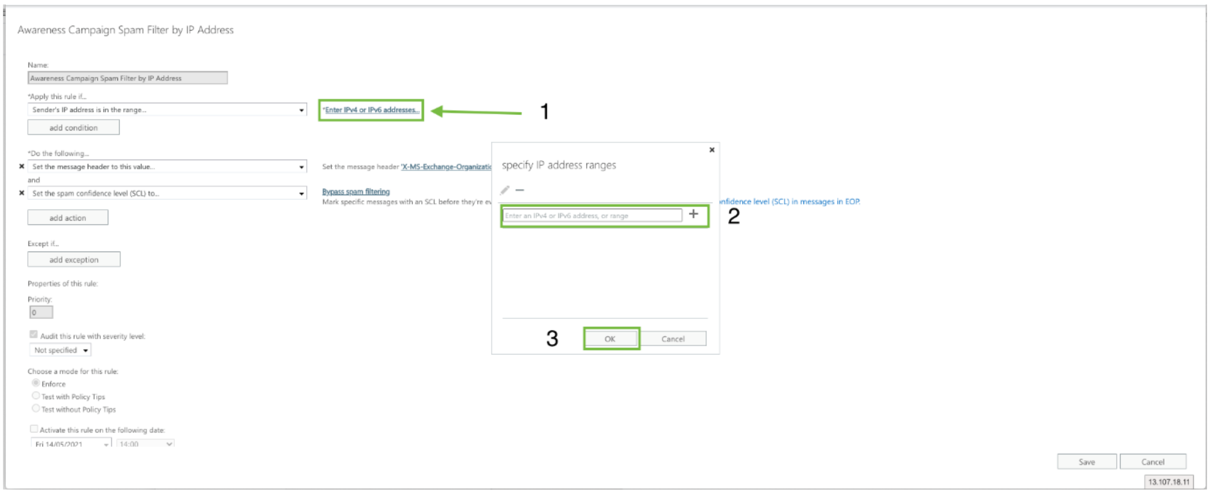
Choose a mode for this rule: ● Enforce ○ Test with Policy Tips ○ Test without Policy Tips

□ Activate this rule on the following date: Fri 14/05/2021 12:30

□ Deactivate this rule on the following date:

1
2
3
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
even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.
Properties of this rule:
Save
Cancel
13.107.18.11

4. Click "Enter IPv4 or IPv6 addresses..." and enter
   a. 104.130.122.237
   b. 159.135.224.107
5. 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

*Apply this rule if... Sender's IP address is in the range...

*Do the following... Set the message header to this value... and Set the spam confidence level (SCL) to...

Set the message header 'X-MS-Exchange-Organizatio

Bypass spam filtering

Mark specific messages with an SCL before they're ev

Priority: 0

Audit this rule with severity level: Not specified

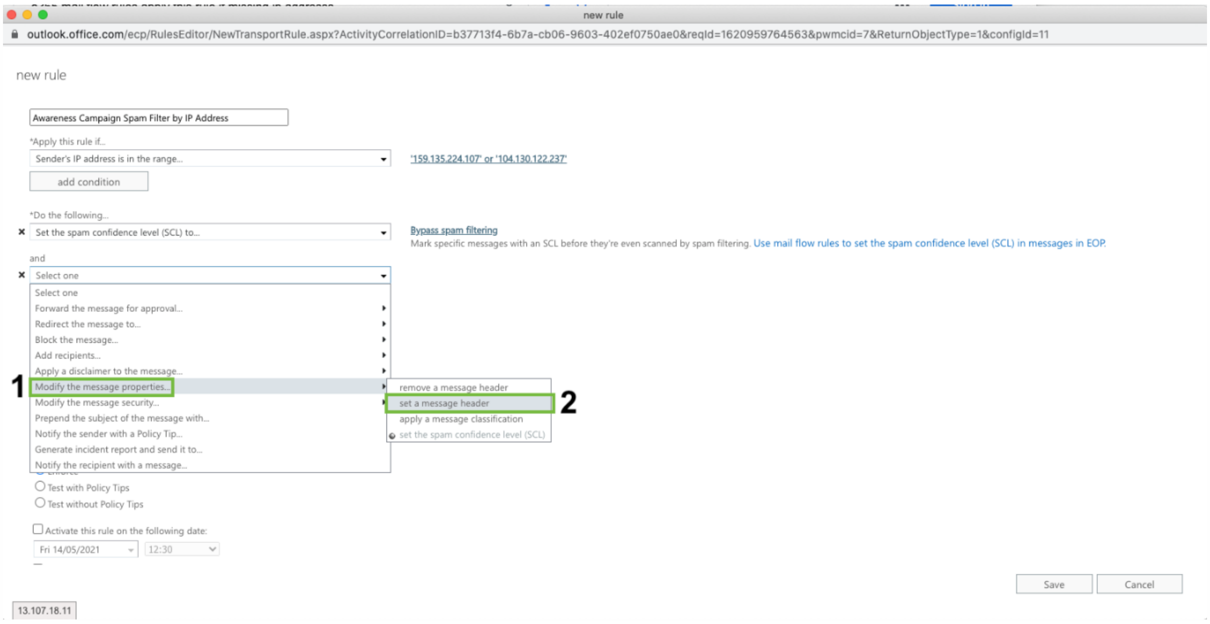
Choose a mode for this rule: ● Enforce ○ Test with Policy Tips ○ Test without Policy Tips

□ Activate this rule on the following date: Fri 14/05/2021 14:00

*Enter IPv4 or IPv6 addresses...
1
add condition
add action
Except if...
add exception
Properties of this rule:
specify IP address ranges
Enter an IPv4 or IPv6 address, or range
+
2
3
OK
Cancel
nfidence level (SCL) in messages in EOP.
Save
Cancel
13.107.18.11

6. Add a message header

   a. Click Add Action
   b. Click ‘Modify the message properties’ > ‘Set a Message Header'



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

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'

*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.

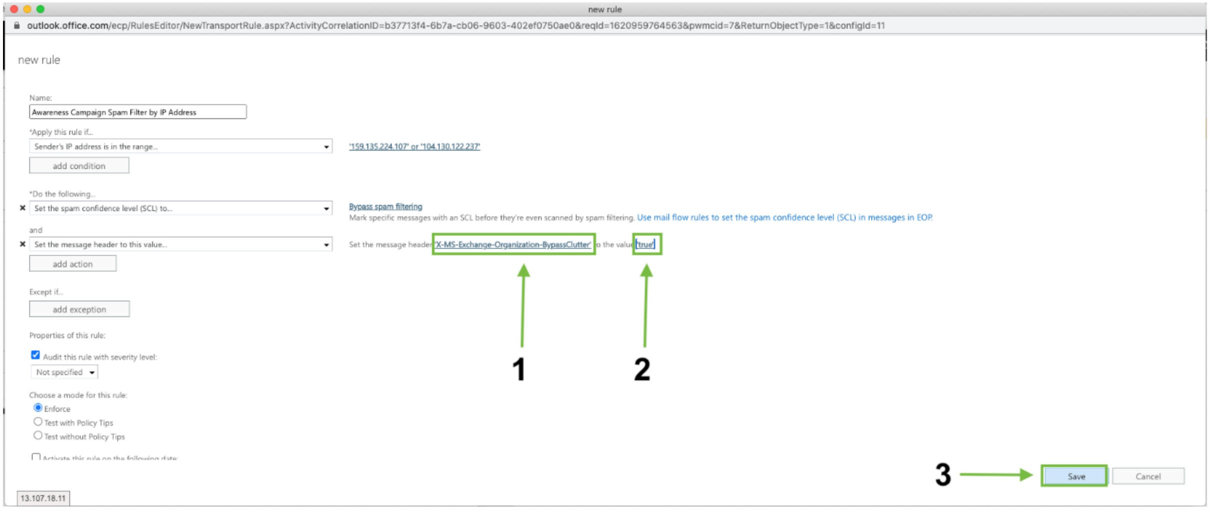
and
Select one

Activate this rule on the following date: Fri 14/05/2021 12:30

13.107.18.11

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...
Notify the sender with a Policy Tip...
Generate incident report and send it to...
Notify the recipient with a message...
remove a message header
set a message header
apply a message classification
set the spam confidence level (SCL)
Test with Policy Tips
Test without Policy Tips
1
2
Save
Cancel

7. 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



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

Name:
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'

*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
Set the message header to this value... Set the message header 'X-MS-Exchange-Organization-BypassClutter' to the value 'true'

Except if...

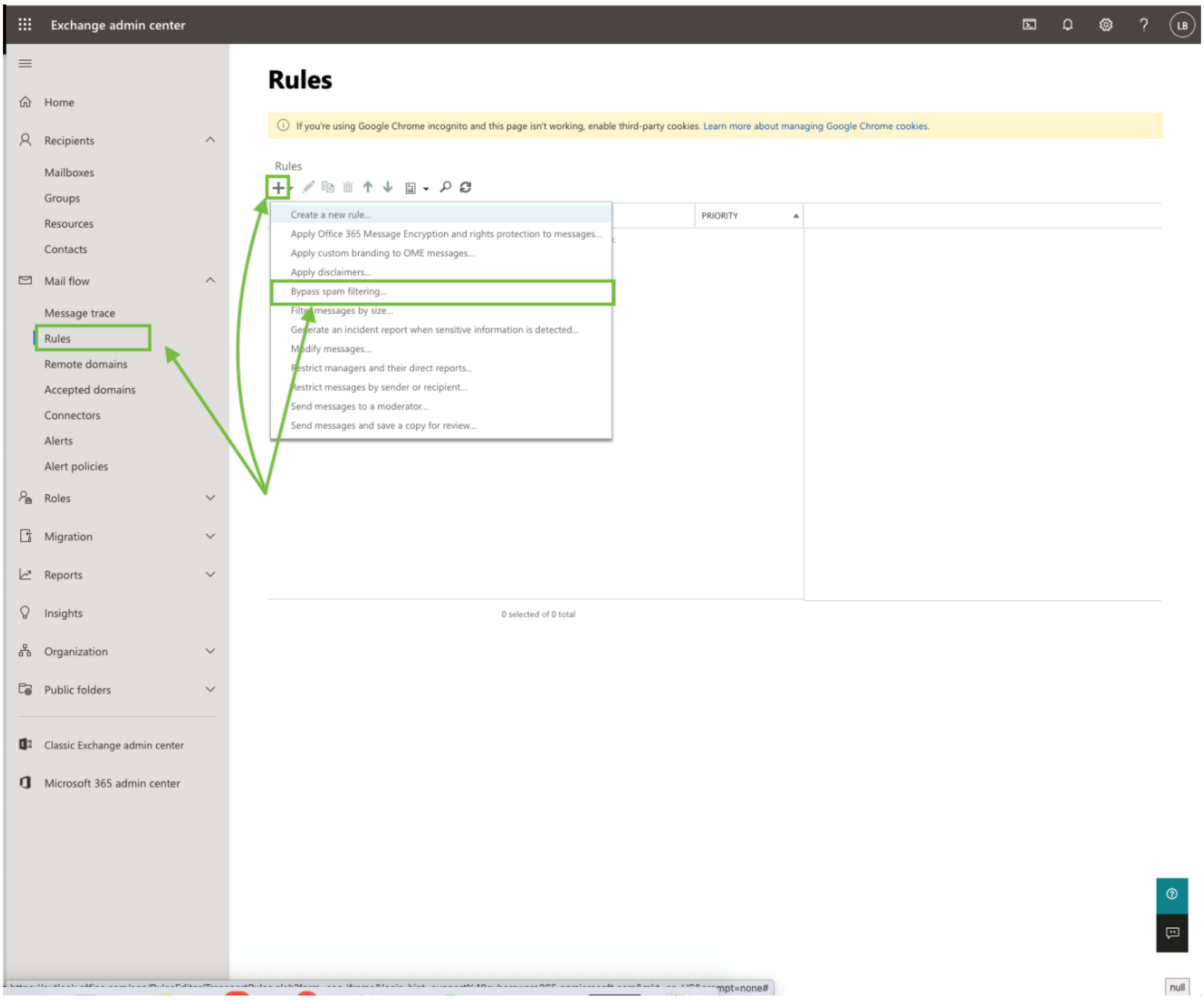
Properties of this rule:
☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

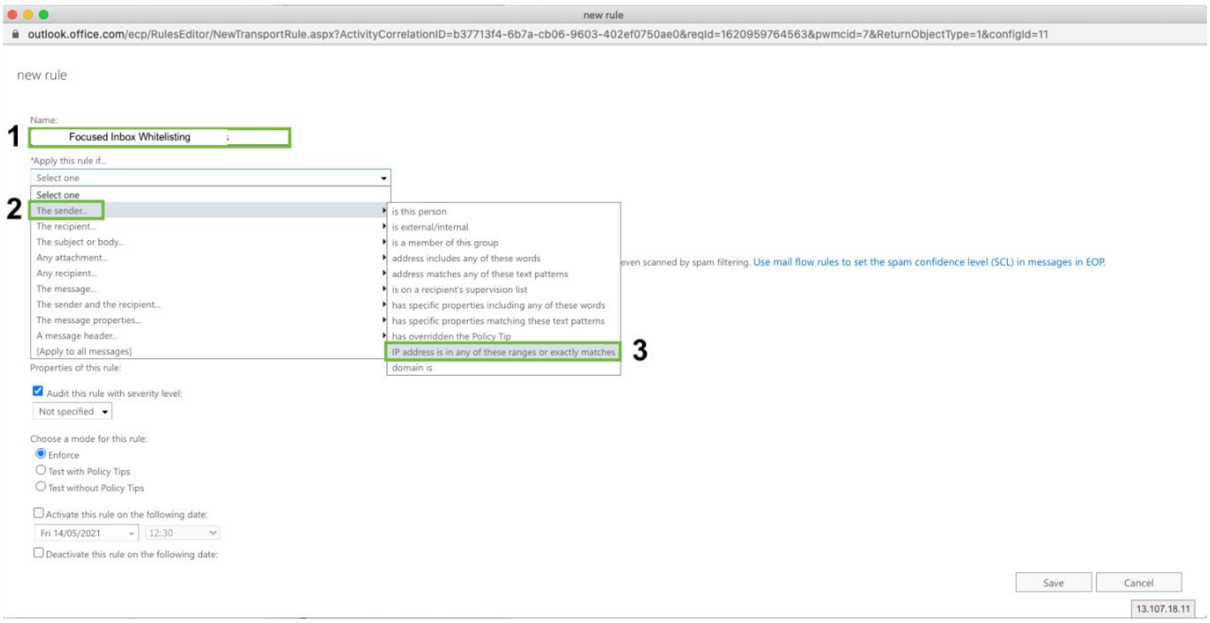
13.107.18.11

Add Mail Flow Rule to bypass focused inbox

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


Exchange admin center
Home
Recipients
Mailboxes
Groups
Resources
Contacts
Mail flow
Message trace
Rules
Remote domains
Accepted domains
Connectors
Alerts
Alert policies
Roles
Migration
Reports
Insights
Organization
Public folders
Classic Exchange admin center
Microsoft 365 admin center
Rules
If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. Learn more about managing Google Chrome cookies.
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...
PRIORITY
0 selected of 0 total
null

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*



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

Name: Focused Inbox Whitelisting

*Apply this rule if... 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

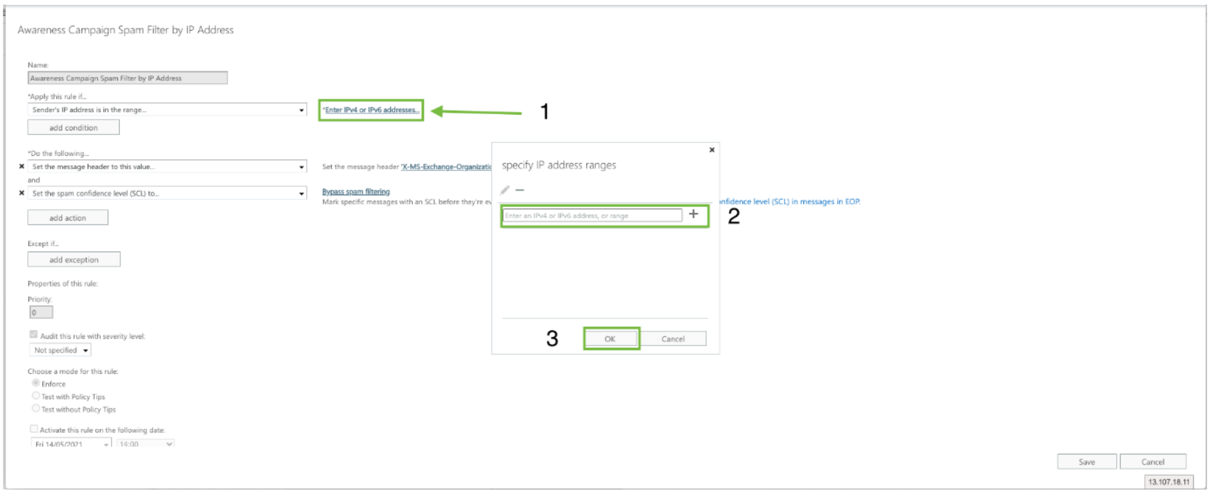
□ Activate this rule on the following date: Fri 14/05/2021 12:30

□ Deactivate this rule on the following date:

...even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

1
2
3
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
Save
Cancel
13.107.18.11

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

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

*Do the following...

Set the message header to this value... Set the message header 'X-MS-Exchange-Organizatio...

and

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

Mark specific messages with an SCL before they're ev... ...nfidence level (SCL) in messages in EOP.

Except if...

Properties of this rule:

Priority: 0

☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:

● Enforce

○ Test with Policy Tips

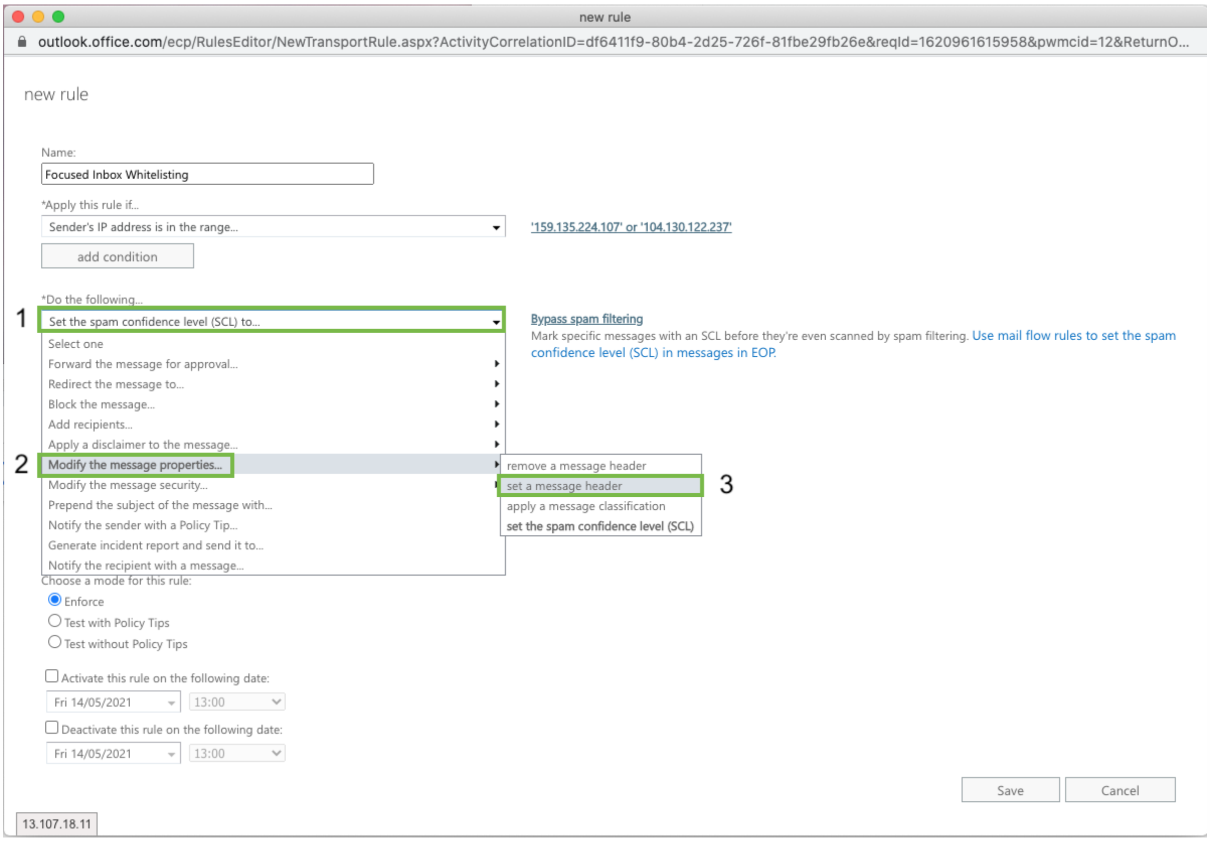
○ Test without Policy Tips

□ Activate this rule on the following date: Fri 14/05/2021 14:00

specify IP address ranges

Enter an IPv4 or IPv6 address, or range

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



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=df6411f9-80b4-2d25-726f-81fbe29fb26e&reqId=1620961615958&pwmcid=12&ReturnO...

new rule

Name:
Focused Inbox Whitelisting

*Apply this rule if...
Sender's IP address is in the range... '159.135.224.107' or '104.130.122.237'

*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.

Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

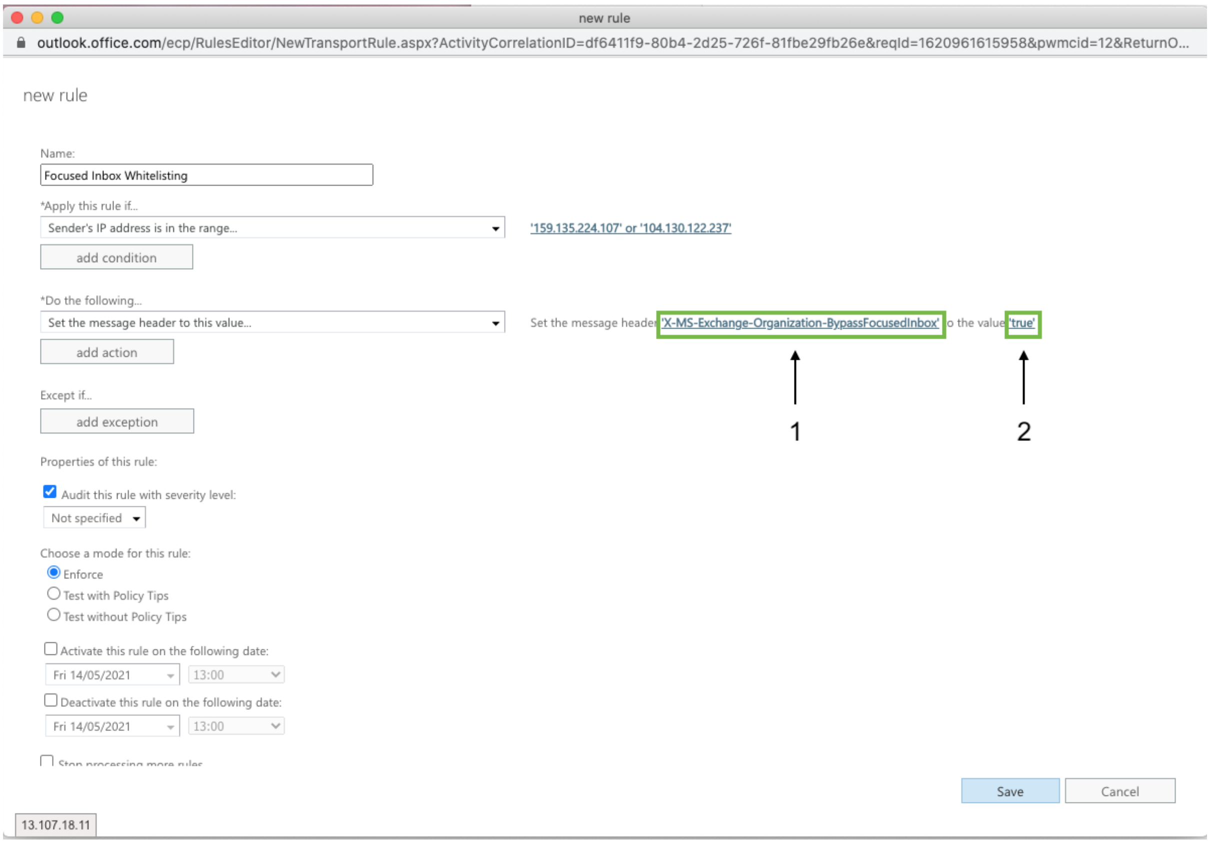
□ Activate this rule on the following date:
Fri 14/05/2021 13:00

□ Deactivate this rule on the following date:
Fri 14/05/2021 13:00

13.107.18.11

add condition
1
Select one
Forward the message for approval...
Redirect the message to...
Block the message...
Add recipients...
Apply a disclaimer to the message...
2
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
set a message header
apply a message classification
set the spam confidence level (SCL)
3
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-BypassFocusedInbox
    b. Click on ... to the value **“Enter text…”** and add (case sensitive!):
        a. true



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=df6411f9-80b4-2d25-726f-81fbe29fb26e&reqId=1620961615958&pwmcid=12&ReturnO...

new rule

Name:
Focused Inbox Whitelisting

*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 message header to this value... Set the message header 'X-MS-Exchange-Organization-BypassFocusedInbox' to the value 'true'

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

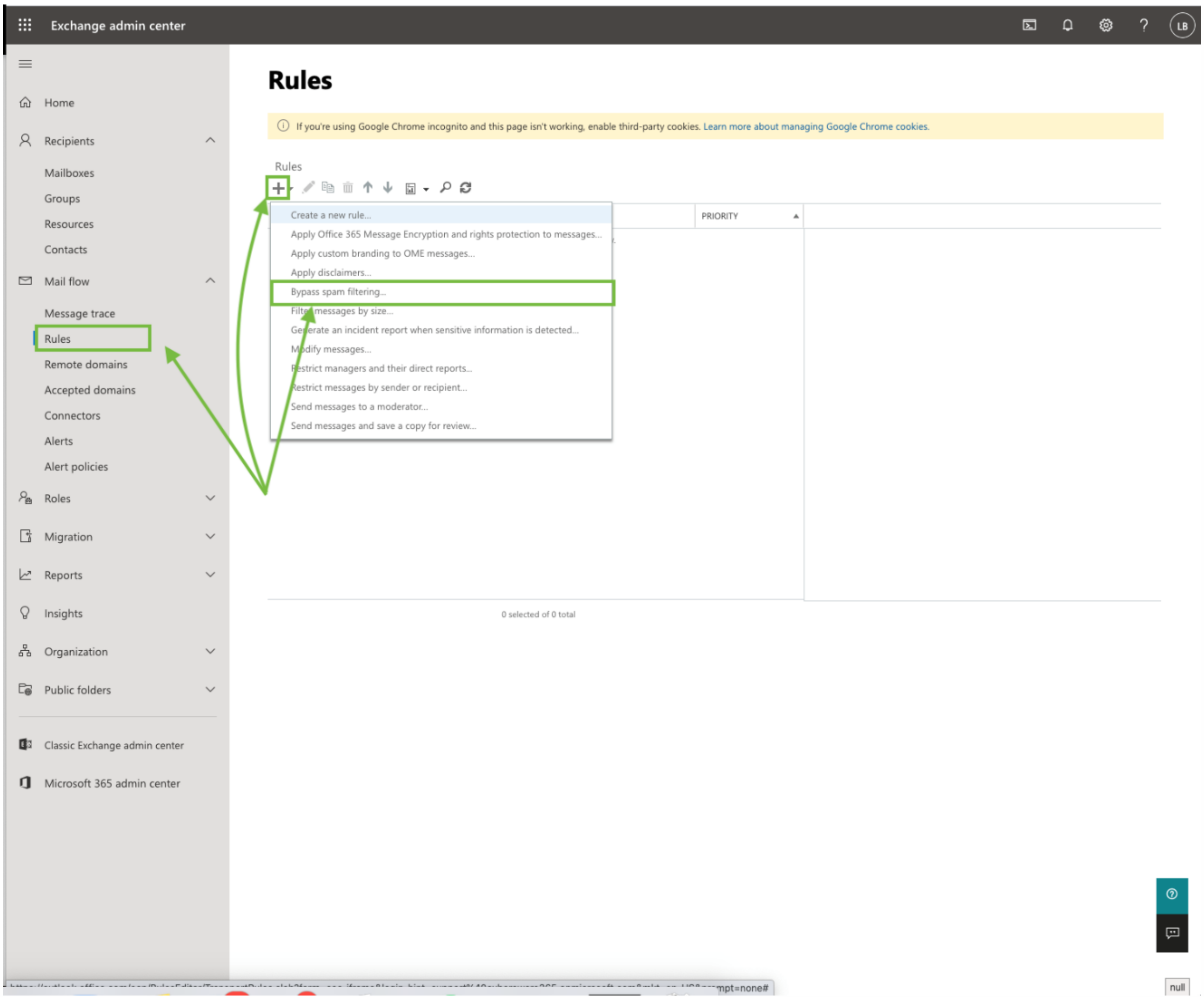
□ Activate this rule on the following date:
Fri 14/05/2021 13:00

□ Deactivate this rule on the following date:
Fri 14/05/2021 13:00

□ Stop processing more rules

Add Mail Flow rule to skip junk filtering

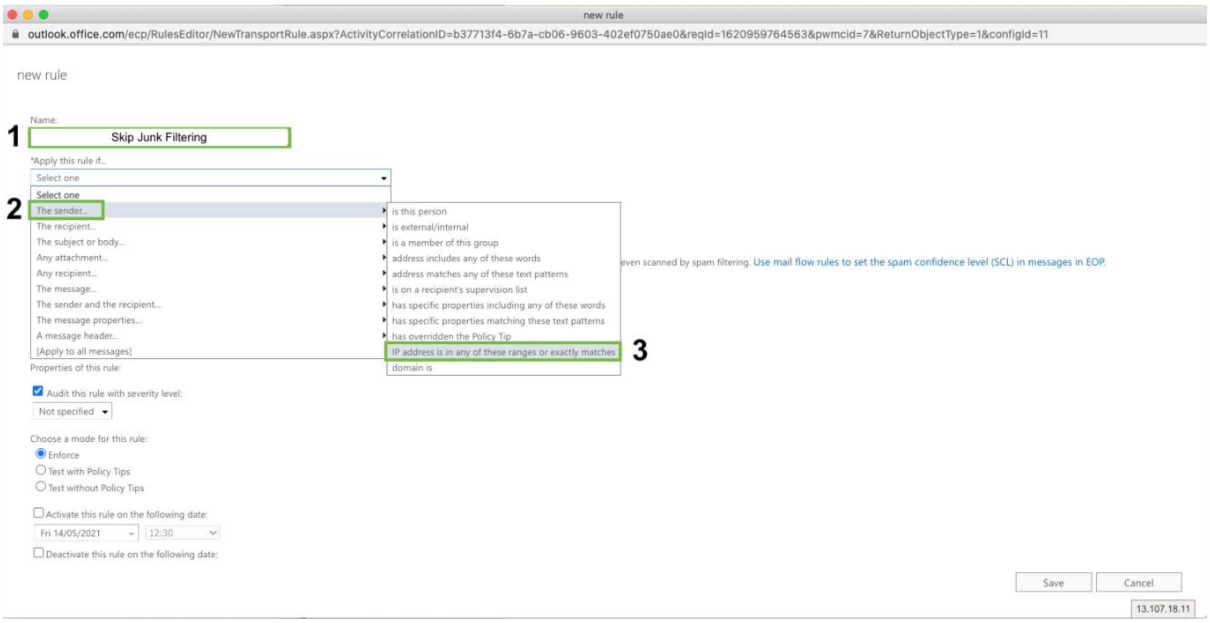
1. Go to Mail Flow > Rules
    a. Create a Bypass Spam Filtering Rule



Exchange admin center
LB
Home
Recipients
Mailboxes
Groups
Resources
Contacts
Mail flow
Message trace
Rules
Remote domains
Accepted domains
Connectors
Alerts
Alert policies
Roles
Migration
Reports
Insights
Organization
Public folders
Classic Exchange admin center
Microsoft 365 admin center
Rules
Rules
PRIORITY
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...
0 selected of 0 total
null

If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. Learn more about managing Google Chrome cookies.

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*



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

new rule

Name:
Skip Junk Filtering

*Apply this rule if...
Select one

even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

Properties of this rule:

☑ Audit this rule with severity level:
Not specified

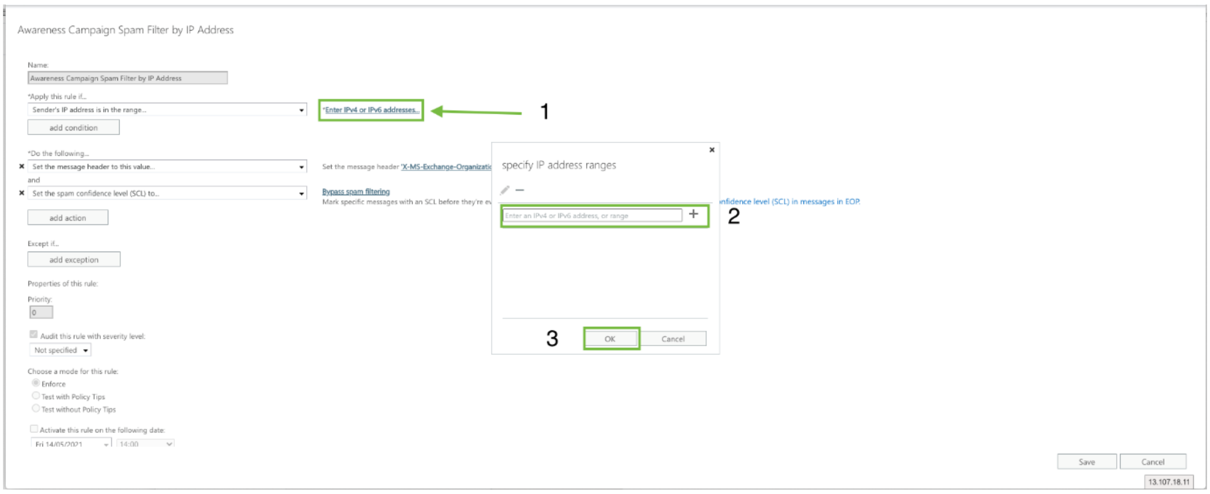
Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date:
Fri 14/05/2021 12:30

□ Deactivate this rule on the following date:

1
2
3
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
Save
Cancel
13.107.18.11

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

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

*Do the following...
Set the message header to this value... Set the message header 'X-MS-Exchange-Organizatio
and
Set the spam confidence level (SCL) to... Bypass spam filtering
Mark specific messages with an SCL before they're ev ...nfidence level (SCL) in messages in EOP.

Except if...

Properties of this rule:

Priority:
0

☑ Audit this rule with severity level:
Not specified

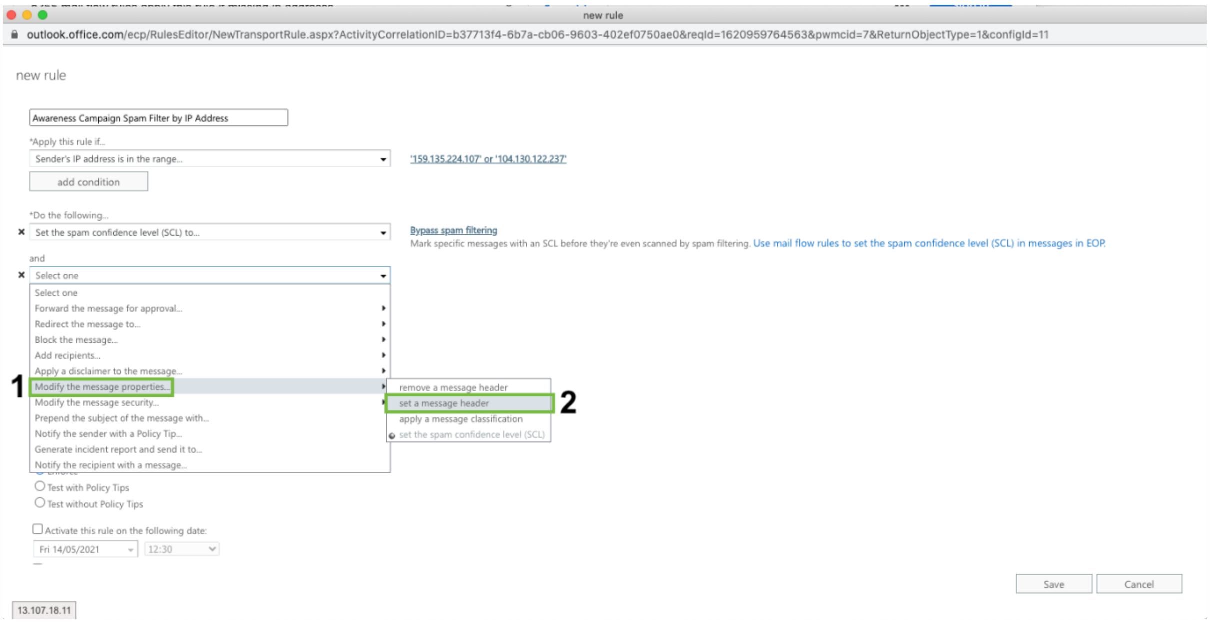
Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date:
Fri 14/05/2021 14:00

specify IP address ranges

Enter an IPv4 or IPv6 address, or range

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



outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

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'

*Do the following...

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

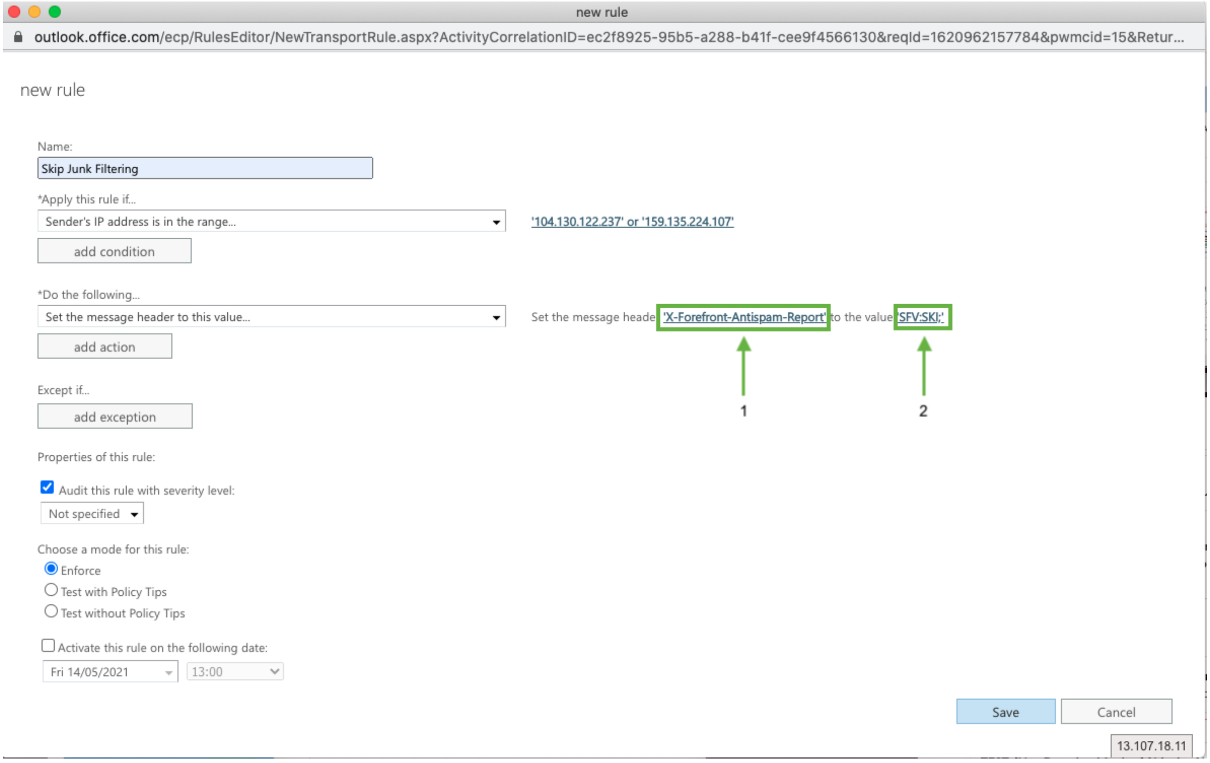
Mark specific messages with an SCL before they're even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

and

Select one

add condition
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
set a message header
2
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
13.107.18.11

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;



outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=ec2f8925-95b5-a288-b41f-cee9f4566130&reqId=1620962157784&pwmcid=15&Retur...

new rule

Name:
Skip Junk Filtering

*Apply this rule if...
Sender's IP address is in the range... '104.130.122.237' or '159.135.224.107'

*Do the following...
Set the message header to this value... Set the message heade 'X-Forefront-Antispam-Report' to the value 'SFV:SKI;'

Except if...

Properties of this rule:

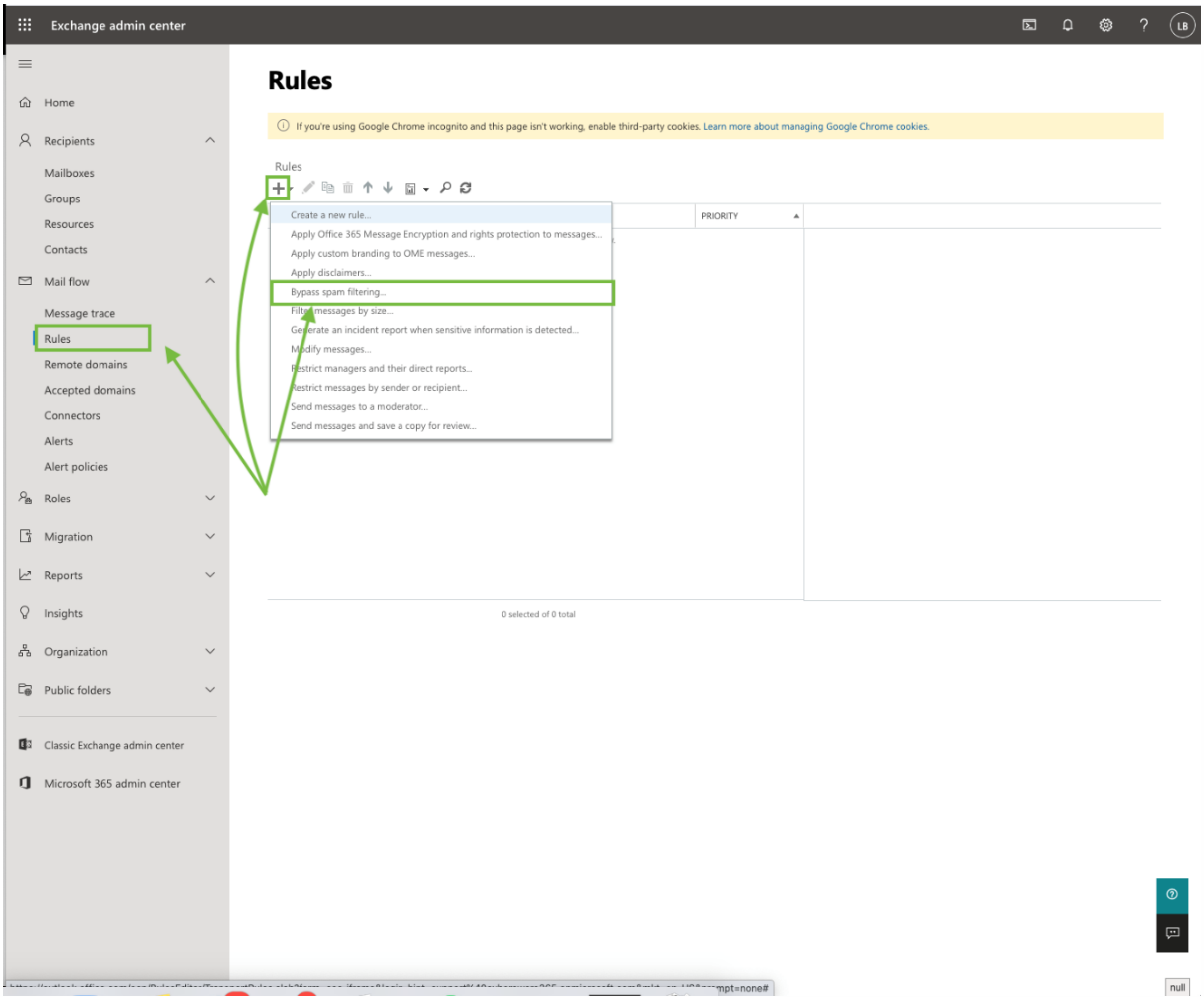
☑ Audit this rule with severity level:
Not specified

Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date:
Fri 14/05/2021 13:00

ATP: Skip Link Scanning

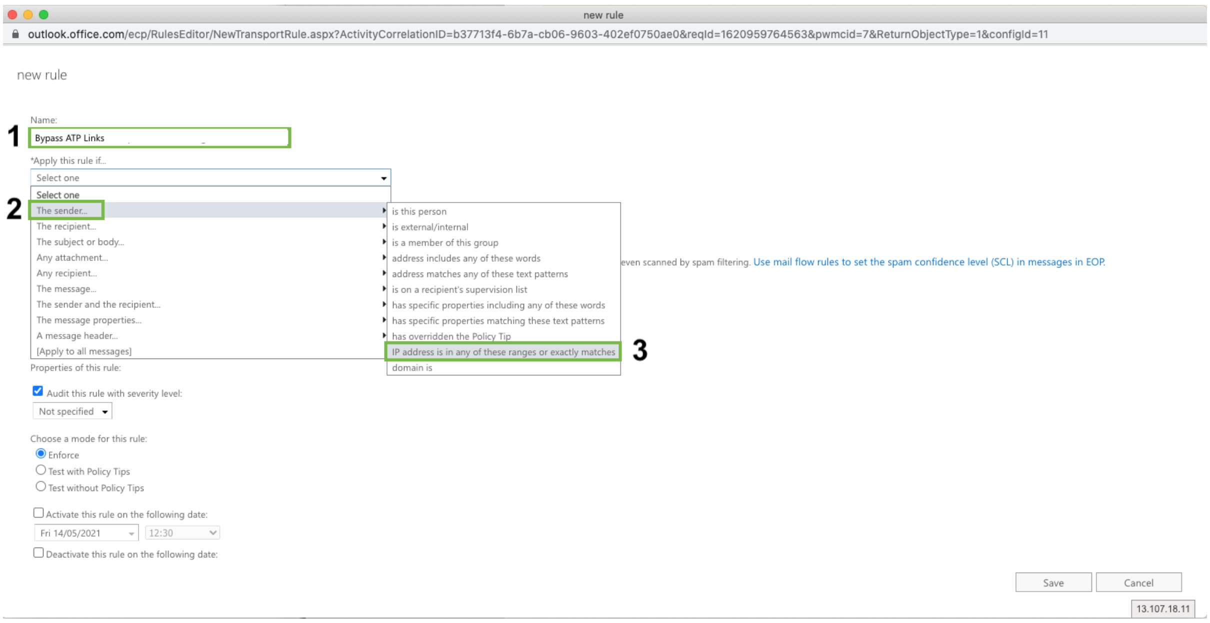
1. Go to Mail Flow > Rules
    a. Create a Bypass Spam Filtering Rule



If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. Learn more about managing Google Chrome cookies.

Exchange admin center
LB
Home
Recipients
Mailboxes
Groups
Resources
Contacts
Mail flow
Message trace
Rules
Remote domains
Accepted domains
Connectors
Alerts
Alert policies
Roles
Migration
Reports
Insights
Organization
Public folders
Classic Exchange admin center
Microsoft 365 admin center
Rules
Rules
PRIORITY
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...
0 selected of 0 total
null

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*



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

Name: Bypass ATP Links

*Apply this rule if... Select one

...even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

Properties of this rule:

☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:

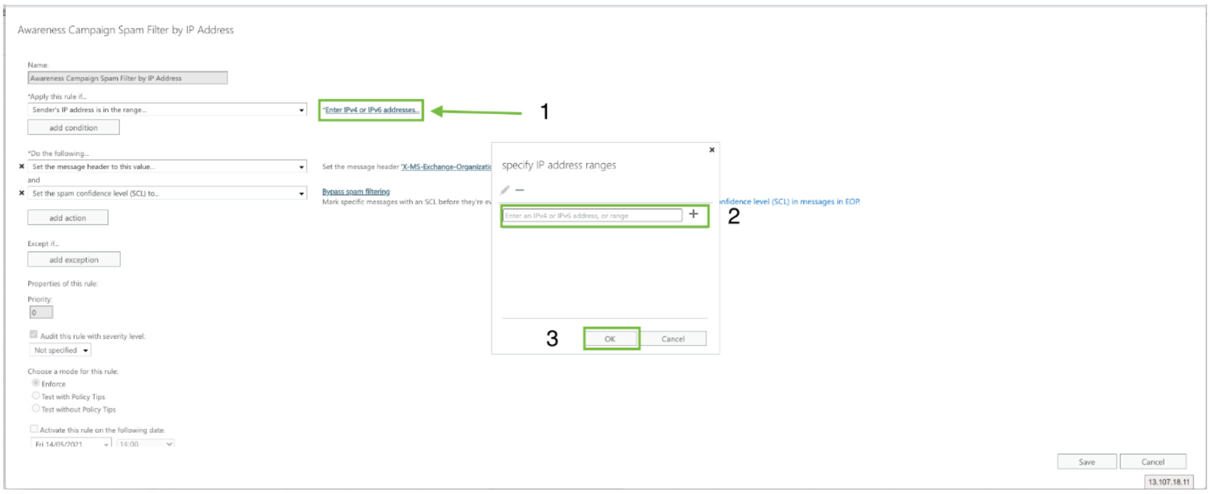
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date: Fri 14/05/2021 12:30

□ Deactivate this rule on the following date:

1
2
3
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
Save
Cancel
13.107.18.11

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

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

*Do the following...
Set the message header to this value... — Set the message header 'X-MS-Exchange-Organizatio...
and
Set the spam confidence level (SCL) to... — Bypass spam filtering
Mark specific messages with an SCL before they're ev... ...nfidence level (SCL) in messages in EOP.

Except if...

Properties of this rule:

Priority: 0

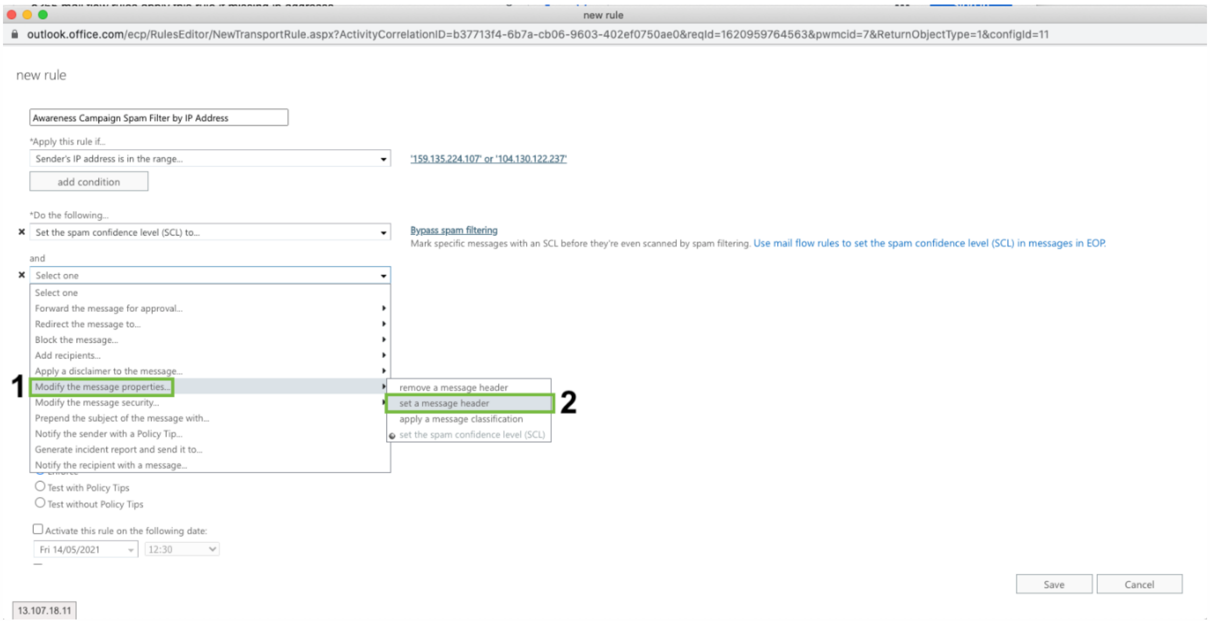
☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:

● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date: Fri 14/05/2021 14:00

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



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

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'

*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

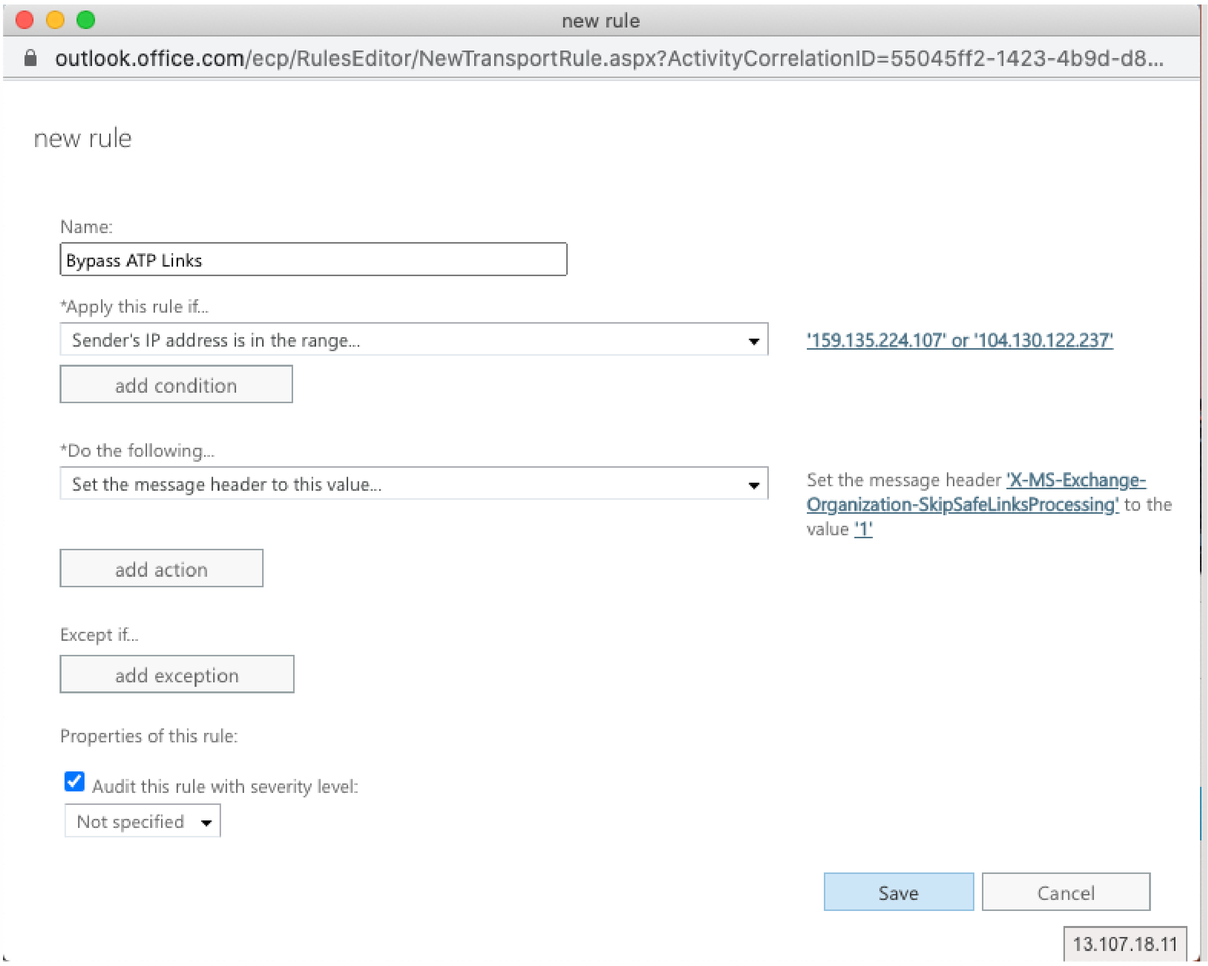
Select one

add condition
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
set a message header
2
apply a message classification
set the spam confidence level (SCL)
○ Test with Policy Tips
○ Test without Policy Tips
Save
Cancel
13.107.18.11

□ Activate this rule on the following date:

Fri 14/05/2021 12:30

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

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=55045ff2-1423-4b9d-d8...

new rule

Name:
Bypass ATP Links

*Apply this rule if...
Sender's IP address is in the range... — '159.135.224.107' or '104.130.122.237'

*Do the following...
Set the message header to this value... — Set the message header 'X-MS-Exchange-Organization-SkipSafeLinksProcessing' to the value '1'

Except if...

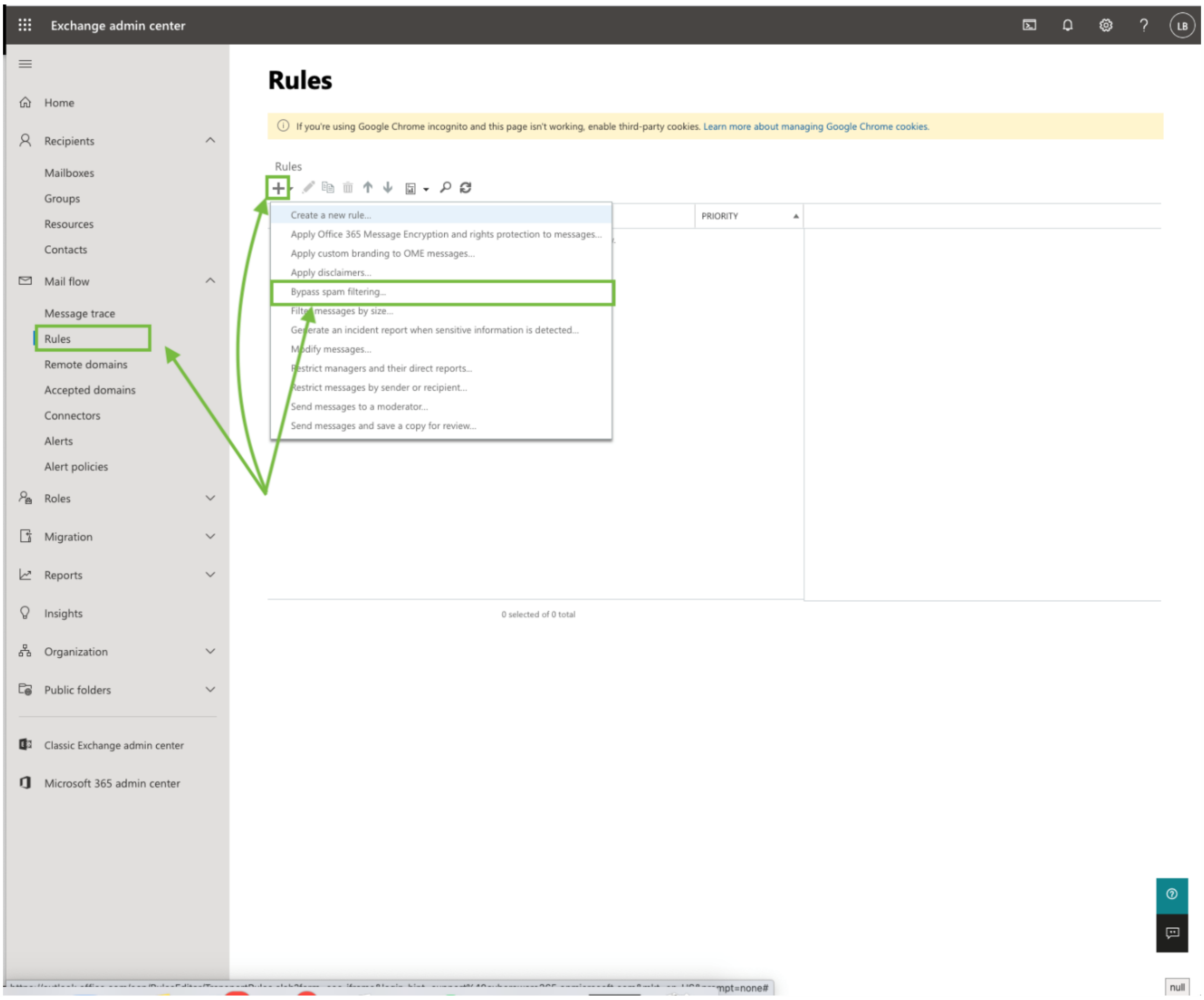
Properties of this rule:

☑ Audit this rule with severity level:
Not specified

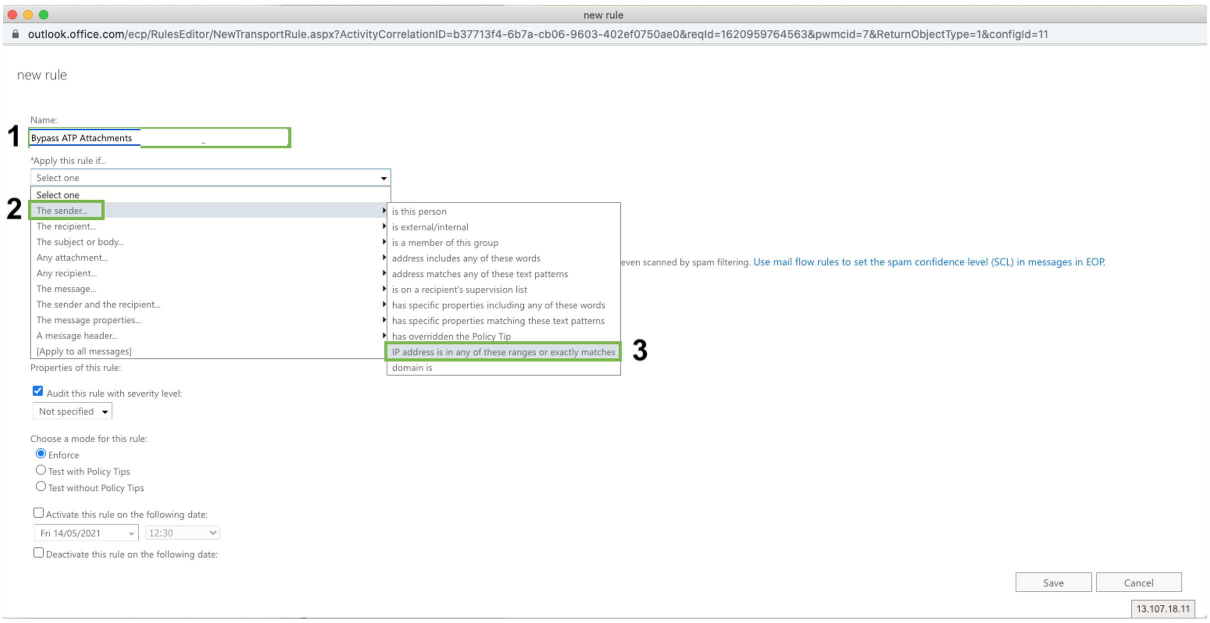
13.107.18.11

ATP: Skip attachment scanning

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


Exchange admin center
Home
Recipients
Mailboxes
Groups
Resources
Contacts
Mail flow
Message trace
Rules
Remote domains
Accepted domains
Connectors
Alerts
Alert policies
Roles
Migration
Reports
Insights
Organization
Public folders
Classic Exchange admin center
Microsoft 365 admin center
Rules
If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. Learn more about managing Google Chrome cookies.
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...
PRIORITY
0 selected of 0 total
null

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

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

Name: Bypass ATP Attachments

*Apply this rule 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...
[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

...even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

Properties of this rule:

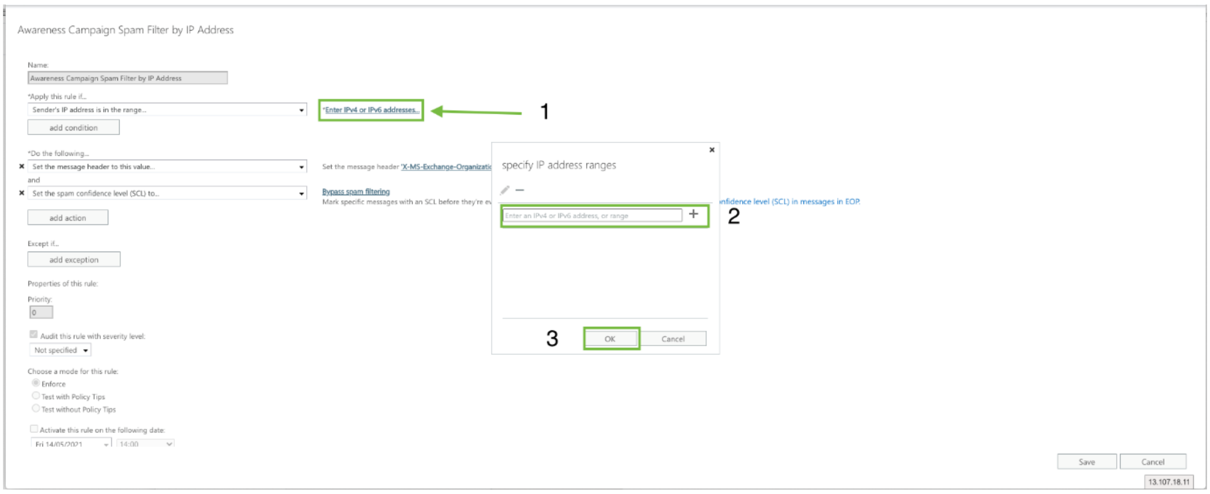
☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date: Fri 14/05/2021 12:30

□ Deactivate this rule on the following date:

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

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

*Do the following...
Set the message header to this value... Set the message header 'X-MS-Exchange-Organizatio...
and
Set the spam confidence level (SCL) to... Bypass spam filtering
Mark specific messages with an SCL before they're ev... ...nfidence level (SCL) in messages in EOP.

Except if...

Properties of this rule:

Priority: 0

☑ Audit this rule with severity level: Not specified

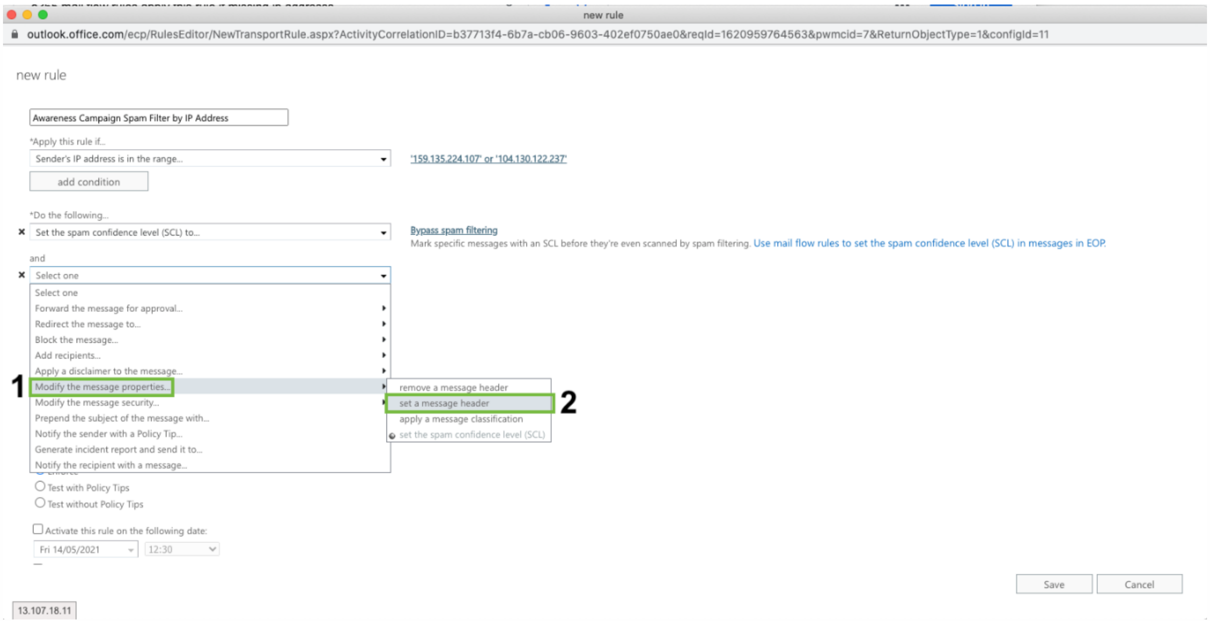
Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date: Fri 14/05/2021 14:00

specify IP address ranges

Enter an IPv4 or IPv6 address, or range

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



new rule

outlook.office.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=b37713f4-6b7a-cb06-9603-402ef0750ae0&reqId=1620959764563&pwmcid=7&ReturnObjectType=1&configId=11

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'

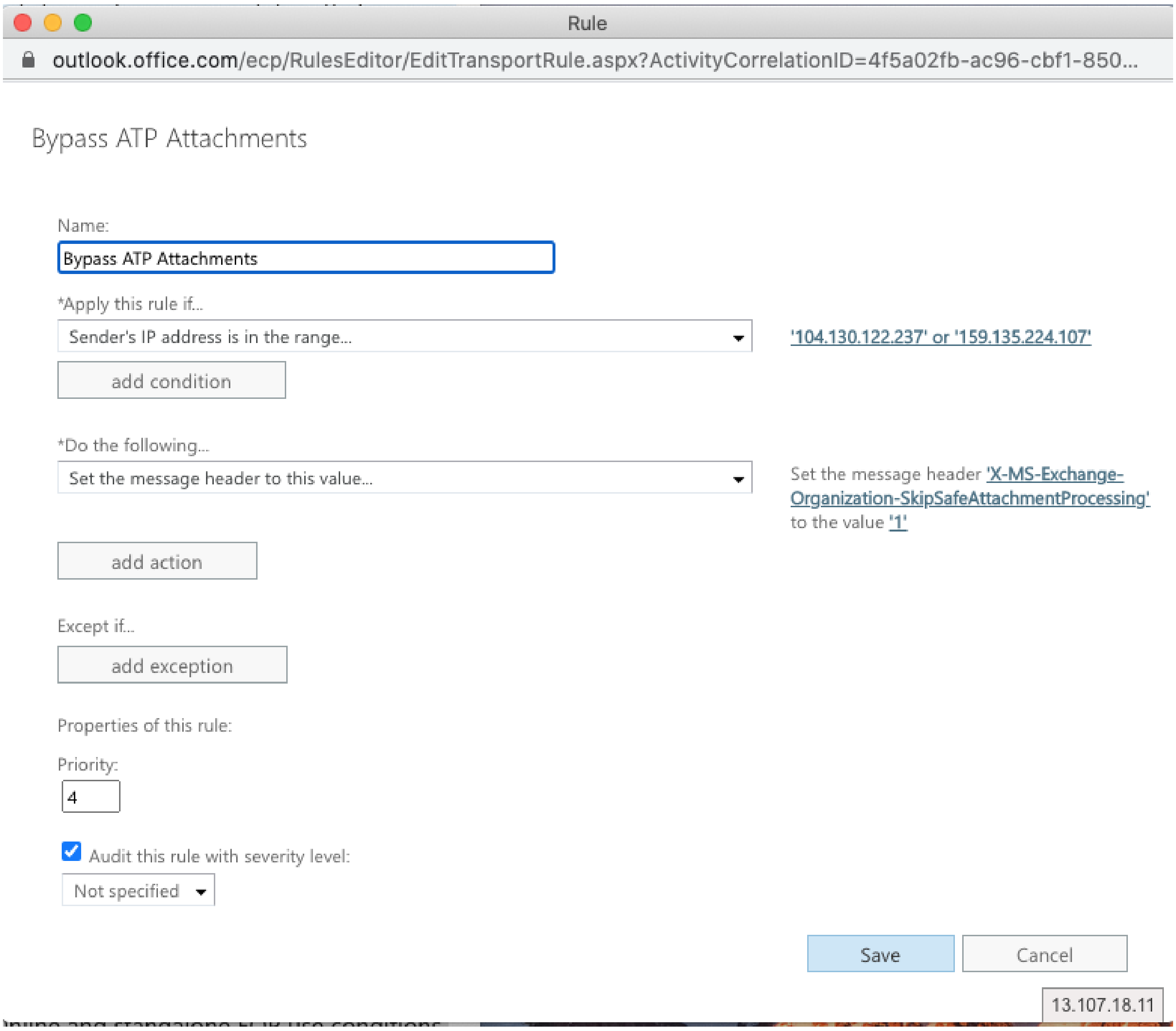
*Do the following...: Set the spam confidence level (SCL) to... Bypass spam filtering

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

add condition
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
set a message header
2
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
13.107.18.11

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



Rule
outlook.office.com/ecp/RulesEditor/EditTransportRule.aspx?ActivityCorrelationID=4f5a02fb-ac96-cbf1-850...

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'

*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