UnsubCentral

Relay Setup

UnsubCentral

Configuration Details

Note: Section below needs to be updated with details for your organization provided during the start-up process (in green)

O365 info needed by USC: < your-account.mail.protection.outlook.com >

USC Smart Host
Stage: < email.compliance-stg.unsubcentral.com >
Prod: < email.compliance.unsubcentral.com >

Outbound Header
Header: < X-ZUAPI-YOUCLIENTID >
Header Value: < YOUR API KEY >

Inbound Header
Header: < X-ZUAPI-Mailclass >
Header Value: < ZH_UCentral >

SSL Subject Name: < *.compliance.unsubcentral.com >

SPF Record
Add to existing SPF in DNS: include:spf.email.compliance.unsubcentral.com

Commented [RP1]: Something similar should be setup so that the client can include on their SPF record to keep in compliance and avoid spam flagging

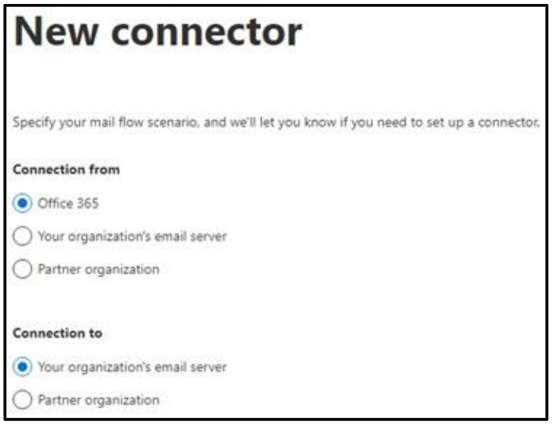
USC IPs < 96.47.24.120/32, 96.47.24.120/32, 96.47.20.90/32, 96.47.24.90/32 >

UnsubCentral

Part 1 – Setup USC Outbound Path

Outbound Connector

1. Create Outbound Connector in O365
   1.1. Open the O365 Exchange Admin Console and go to **Mail Flow** > **Connectors** (https://admin.exchange.microsoft.com/#/connectors)
   1.2. Create a new Outbound Connector from Office 365 to Your Organization’s email server, then click **Next**



New connector

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

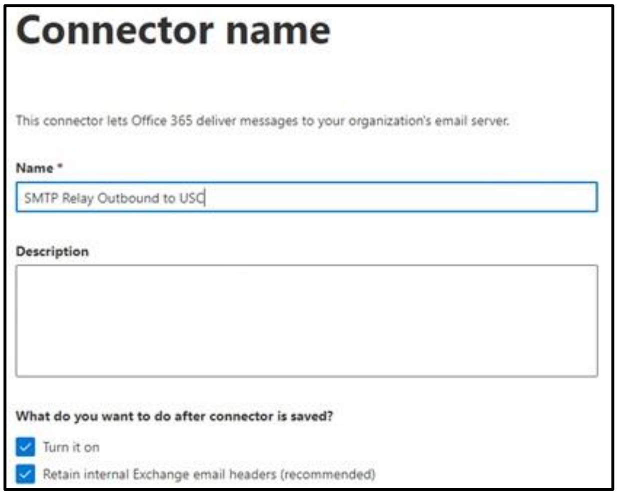
Connection from

● Office 365
○ Your organization's email server
○ Partner organization

Connection to

● Your organization's email server
○ Partner organization

   1.3. Give the Outbound Connector a descriptive name
   1.4. Select both check boxes and then click **Next**



Connector name

This connector lets Office 365 deliver messages to your organization's email server.

Name *

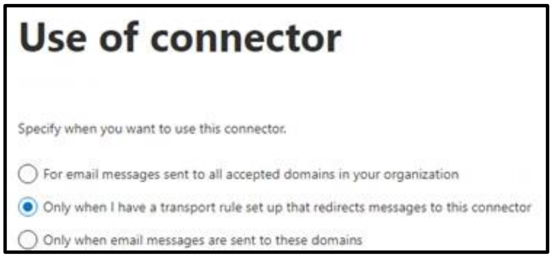
SMTP Relay Outbound to USC

Description

What do you want to do after connector is saved?

☑ Turn it on
☑ Retain internal Exchange email headers (recommended)

1.5. Select **Only when I have a transport rule set up that redirects messages to this connector**, then click **Next**



Use of connector

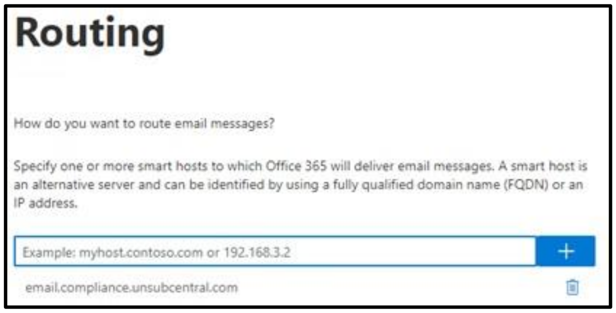
Specify when you want to use this connector.

○ For email messages sent to all accepted domains in your organization

● Only when I have a transport rule set up that redirects messages to this connector

○ Only when email messages are sent to these domains

1.6. Select **Route mail through this smart host** and enter the appropriate USC Smart Host listed at the beginning of this document and then click the '**+**' to add it. Click **Next**



Routing

How do you want to route email messages?

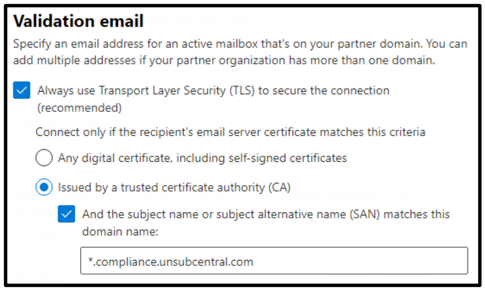
Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address.

Example: myhost.contoso.com or 192.168.3.2 +

email.compliance.unsubcentral.com

1.7. Select the options below and add the following domain name (do not include <> or spaces), then click **Next**

1.7.1. < *.compliance.unsubcentral.com >



Validation email

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

☑ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

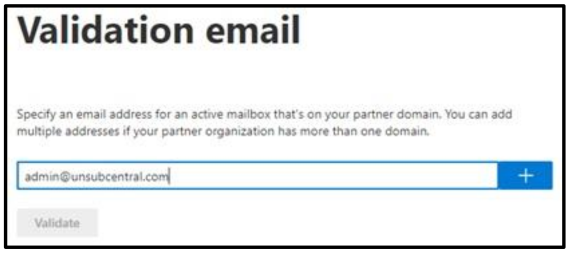
○ Any digital certificate, including self-signed certificates

● Issued by a trusted certificate authority (CA)

☑ And the subject name or subject alternative name (SAN) matches this domain name:

*.compliance.unsubcentral.com

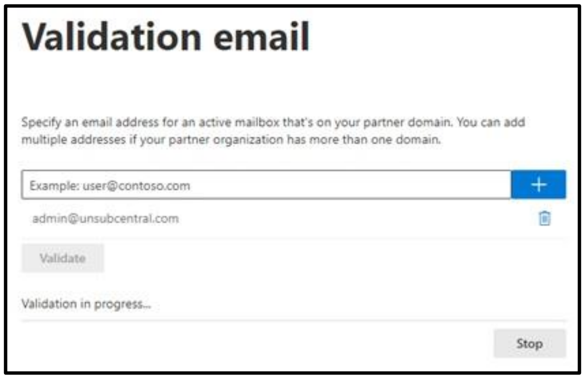
1.8. You will need to validate that the Smart Host is accepting your emails. Add an appropriate address and click the '**+**' to add it.


Validation email

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

admin@unsubcentral.com

1.9. Then click the Validate button to verify that the connector works.


Validation email

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

Example: user@contoso.com

admin@unsubcentral.com

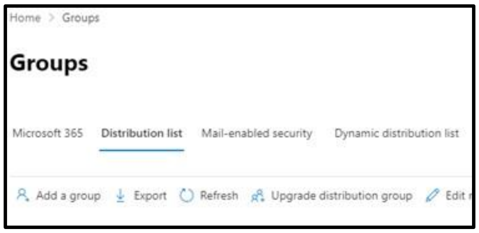
Validation in progress...

1.10. If it completes successfully, click Next to add it. If not, verify that the settings are correct and that UnsubCentral is ready to receive emails from your domain.

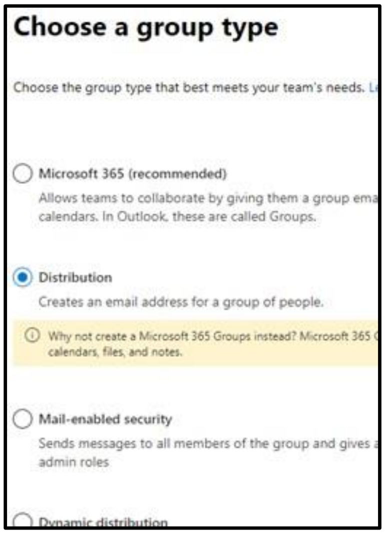
Commented [RP2]: USC needs to add the ability for the smarthost to accept an email that does not have a client code. Maybe restrict it to receiving for a single address? Validate@unsubcentral.com, or something similar?

Distribution or Security Group

2. Create a dedicated a Distribution Group or Mail Enabled Security Group for senders that should use the USC system. We'll use a Distribution Group in our example
   2.1. Open the O365 Exchange Admin Console and go to Recipients > Groups (https://admin.exchange.microsoft.com/#/groups)
   2.2. Select **Add Group**



2.3. Select **Distribution**, then click **Next**



Choose a group type

Choose the group type that best meets your team's needs. L

○ Microsoft 365 (recommended)

Allows teams to collaborate by giving them a group ema calendars. In Outlook, these are called Groups.

● Distribution

Creates an email address for a group of people.

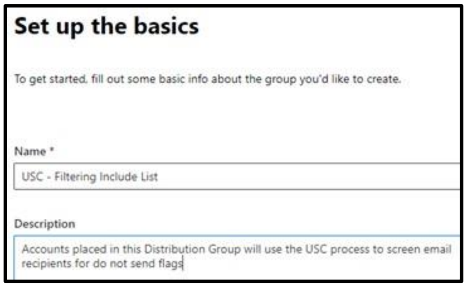
Why not create a Microsoft 365 Groups instead? Microsoft 365 calendars, files, and notes.

○ Mail-enabled security

Sends messages to all members of the group and gives admin roles

○ Dynamic distribution

2.4. Add a descriptive name for the Distribution Group, then click **Next**



Set up the basics

To get started, fill out some basic info about the group you'd like to create.

Name *

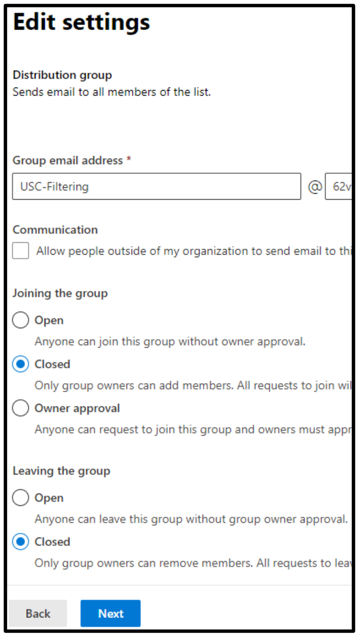
USC - Filtering Include List

Description

Accounts placed in this Distribution Group will use the USC process to screen email recipients for do not send flags

2.5. Add an appropriate email address for the new Distribution Group and select the settings most appropriate for your organization, then click **Next**

2.5.1. NOTE: This Distribution Group will NOT need to receive emails from outside your organization for the USC process



Edit settings

Distribution group
Sends email to all members of the list.

Group email address *
USC-Filtering @ 62v

Communication
☐ Allow people outside of my organization to send email to thi

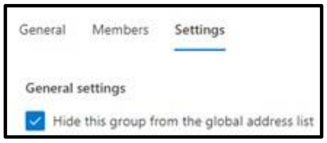
Joining the group
○ Open
Anyone can join this group without owner approval.
● Closed
Only group owners can add members. All requests to join wil
○ Owner approval
Anyone can request to join this group and owners must appr

Leaving the group
○ Open
Anyone can leave this group without group owner approval.
● Closed
Only group owners can remove members. All requests to lea

2.6. Review the settings on the next page, then click **Create Group**

2.7. Search for and open your new Distribution Group

2.8. On the **Settings tab**, you may want to select **Hide this group from the Global Address List**. This is optional and will work either way.



General settings
☑ Hide this group from the global address list

UnsubCentral

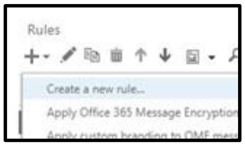
2.9. In the Members tab, select **View and manage members** and then **Add members** to add anyone that should be included in the USC recipient filtering

Outbound Transport Rule

3. Create Outbound Transport Rule

3.1. Open the O365 Exchange Admin Console and go to **Mail Flow** > **Rules** (https://admin.exchange.microsoft.com/#/transportrules)

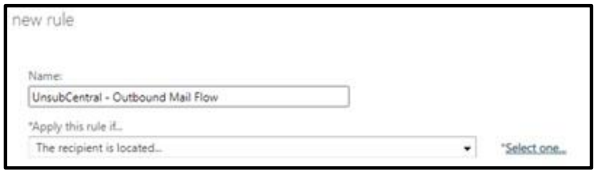
3.2. **Create a New Rule**


Rules
Create a new rule...
Apply Office 365 Message Encryption
Apply custom branding to OME mess

3.3. Add a descriptive name for the Transport Rule

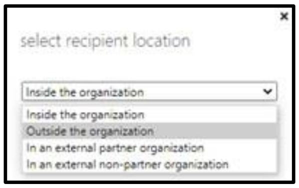
3.4. Under **Apply this rule if…**, add the following Conditions

3.4.1. **The recipient is located…** > **Select one…** > select **Outside the organization**

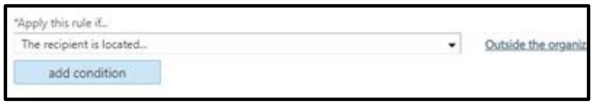

new rule

Name: UnsubCentral - Outbound Mail Flow

*Apply this rule if... The recipient is located... *Select one...

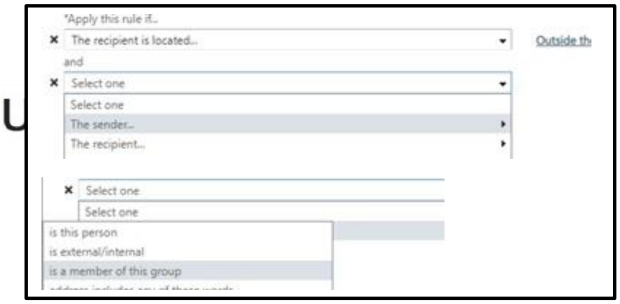

select recipient location
Inside the organization
Inside the organization
Outside the organization
In an external partner organization
In an external non-partner organization

3.4.2. Select **Add Condition** (you may need to select the **More options** at the bottom of the window to add more conditions)

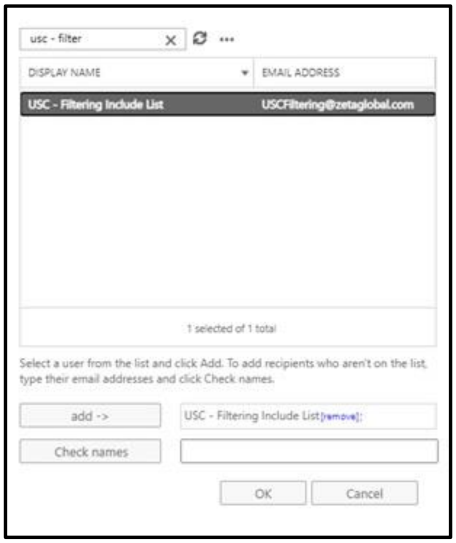

*Apply this rule if... The recipient is located... Outside the organiz

3.4.3. Do the same process to create another Condition for if the Sender is located **Inside the organization**

3.4.4. For the last Condition, select **The Sender…** > **is a Member of this group**


*Apply this rule if... The recipient is located... Outside th

3.4.4.1. Search for and select the Distribution Group created in the previous section, click the **Add** button, then **OK**



DISPLAY NAME	EMAIL ADDRESS
USC - Filtering Include List	USCFiltering@zetaglobal.com

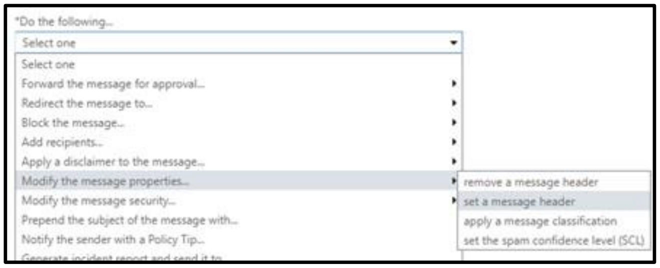
1 selected of 1 total

Select a user from the list and click Add. To add recipients who aren't on the list, type their email addresses and click Check names.

USC - Filtering Include List[remove];

3.5. Under **Do the following…**, add the following Actions

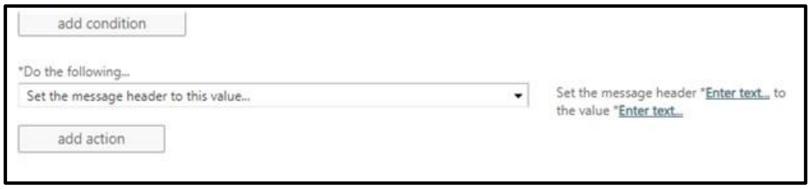
3.5.1. Modify the message properties > **Set a message header**


*Do the following...
Select one
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...
remove a message header
set a message header
apply a message classification
set the spam confidence level (SCL)

3.5.1.1. Select **Enter text** and add the Message Header (do not include <> or spaces):

< X-ZUAPI-YOURCLIENTID >

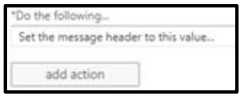
3.5.1.2. Select **Enter text** and add the Header Value (do not include <> or spaces):
< YOUR API KEY >



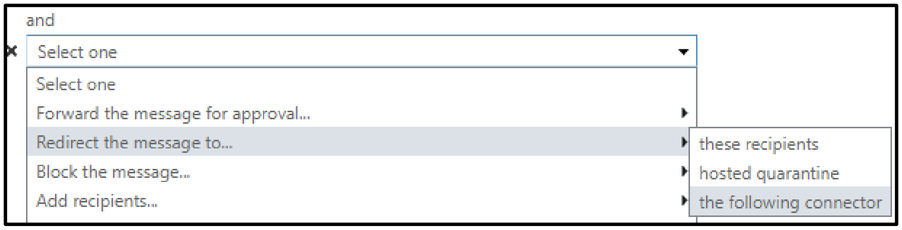
Set the message header to this value...

Set the message header *Enter text... to the value *Enter text...

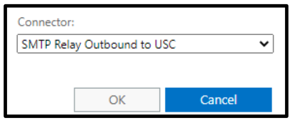
3.5.2. Select **Add Action**



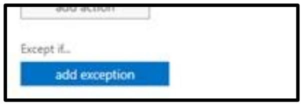
3.5.3. For the next Action, select **Redirect message to** > **the following connector**

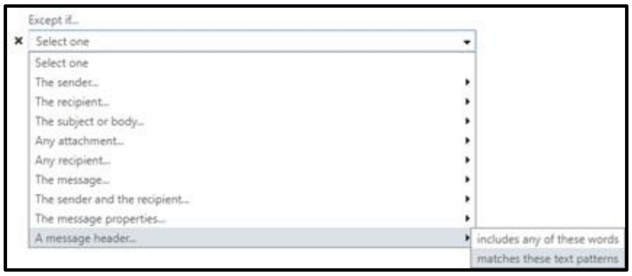


3.5.4. Select Outbound Connector created earlier and click **OK**


Connector: SMTP Relay Outbound to USC

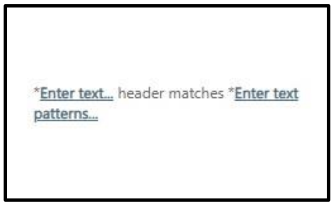
3.6. Add an Exception to identify USC processed emails to prevent looping





3.6.1. Select **Enter text** and add the Message Header (do not include <> or spaces): < X-ZUAPI-Mailclass >

3.6.2. Select **Enter text** and add the Header Value (do not include <> or spaces): **<** ZH_UCentral **>**

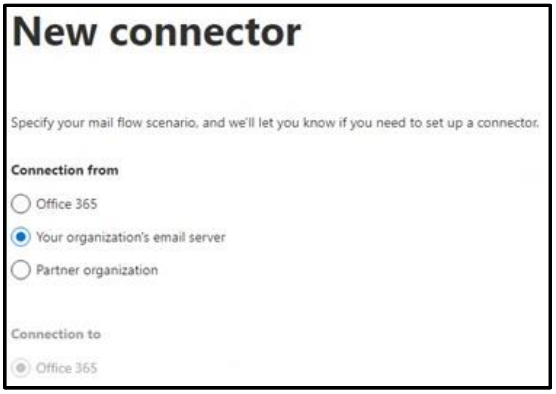


*Enter text... header matches *Enter text patterns...

Part 2 – Setup USC Inbound Path

Inbound Connector

1. Create Inbound Transport Rule
   1.1. In the From section, select **Your organization's email server**. In the To section, **Office 365** will automatically be selected for you



New connector

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

Connection from

○ Office 365

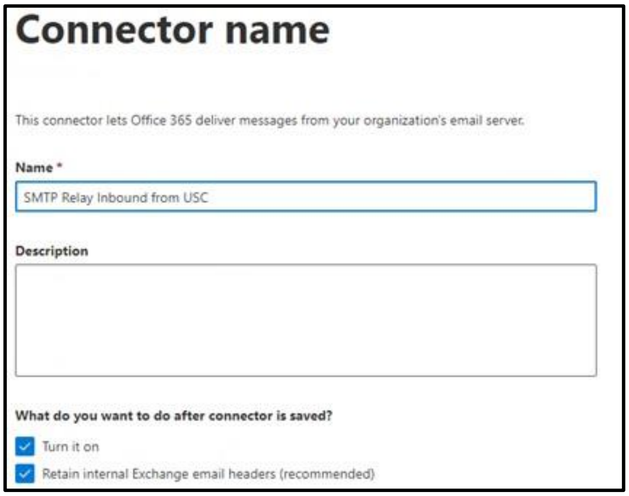
● Your organization's email server

○ Partner organization

Connection to

● Office 365

   1.2. New connector, type the name, in this case we used **SMTP Relay Inbound from USC**. Select both checkboxes at the bottom, and click **Next**.



Connector name

This connector lets Office 365 deliver messages from your organization's email server.

Name *

SMTP Relay Inbound from USC

Description

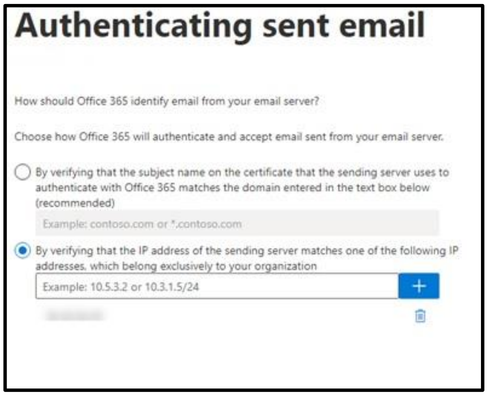
What do you want to do after connector is saved?

☑ Turn it on

☑ Retain internal Exchange email headers (recommended)

1.3. Select **By verifying that the IP address of the sending server matches one of the following IP addresses, which belong exclusively to your organization**. Click the + to add it and click **Next**.

Commented [RP3]: Are we going to use a cert instead of IP's? A cert would be more scalable



Authenticating sent email

How should Office 365 identify email from your email server?

Choose how Office 365 will authenticate and accept email sent from your email server.

○ By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches the domain entered in the text box below (recommended)

Example: contoso.com or *.contoso.com

● By verifying that the IP address of the sending server matches one of the following IP addresses, which belong exclusively to your organization

Example: 10.5.3.2 or 10.3.1.5/24 +

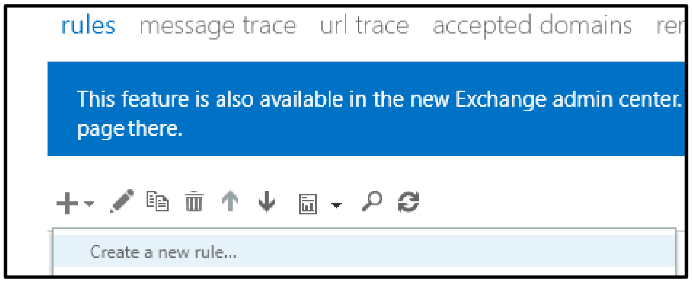
1.4. Click **Create connector**.

Test email by sending from account that is in the Distribution Group above, and from one that is not. Both should reach their destination, but the USC processed email should have a header for <   X-Zeta-Mailclass >

Troubleshooting - Mailer-daemon arriving in Junk

The Mailer-Damon sends NDR emails back to the sender when a recipient is flagged as do not send. If these emails are arriving in your junk folders, you should be able to resolve this with a Transport Rule.

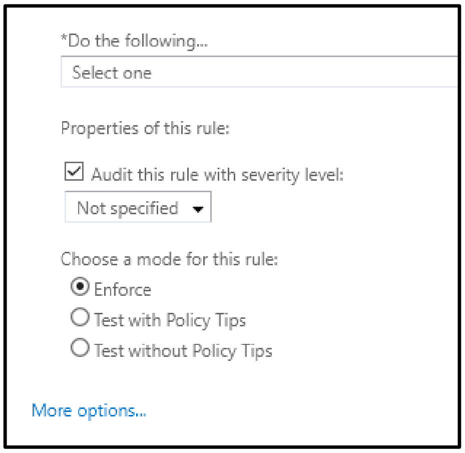
1. Login to Exchange Admin (https://outlook.office365.com/ecp/?rfr=Admin)
    1.1. Click **mail flow**
    1.2. Click **rules**
    1.3. Click the **+** and Select **Create a new rule...**



This feature is also available in the new Exchange admin center. page there.

2. Within the rule, give it a name like **Allow USC bypass spam filtering**

3. In the new window scroll down, and select **More options...**



*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...

4. Scroll, back to the top, under **Apply this rule if...**

4.1. Select **IP address is in any of these ranges or exactly matches**

4.2. Enter the following IP addresses individually and click the **+**:

< 96.47.24.120/32, 96.47.24.120/32, 96.47.20.90/32, 96.47.24.90/32 >

4.3. Click **OK**

5. Click **add condition**

5.1. If this is missing please, read step 3, about selecting **More options...**

6. Select **domain is**, which will output as **The sender's domain is...**

6.1. Add your respective sending domain and click the **+** in this case we're using zetagalactic as a test.

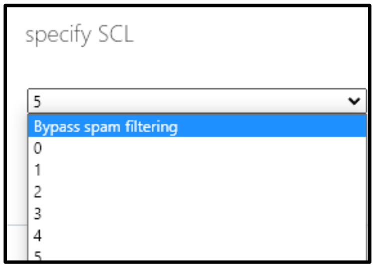
6.2. Click **OK**

7. Under **Do the following...**

7.1. Hover over **Modify the message properties...**

7.1.1. Select **set the spam confidence level (SCL) to...**

7.1.2. Choose **Bypass spam filtering**



specify SCL

5

Bypass spam filtering

0

1

2

3

4

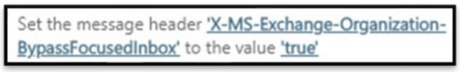
5

8. Click **add condition**

9. Hover over **Modify the message properties...**

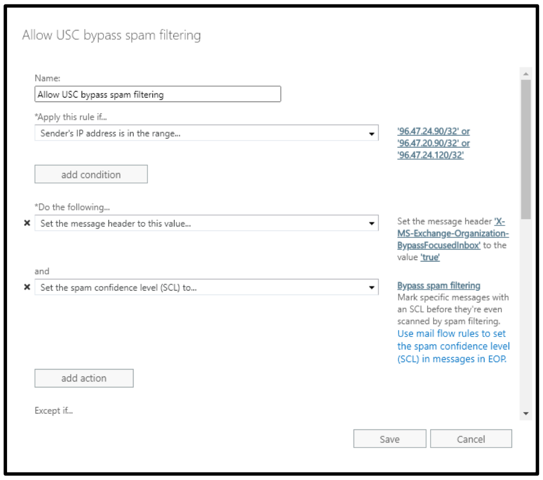
9.1. Select **set a message header**

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



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

10. Click **Save**.
11. The end result should look like this, notice when you select certain rules the name changes.



Allow USC bypass spam filtering

Name:
Allow USC bypass spam filtering

*Apply this rule if...
Sender's IP address is in the range... — '96.47.24.90/32' or '96.47.20.90/32' or '96.47.24.120/32'

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

and
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.

Except if...