

Connectors for Office 365 Setup Guide

To enable **Signatures for Office 365** to apply signatures to your messages you must ensure that your email flows through the Exclaimer Cloud.

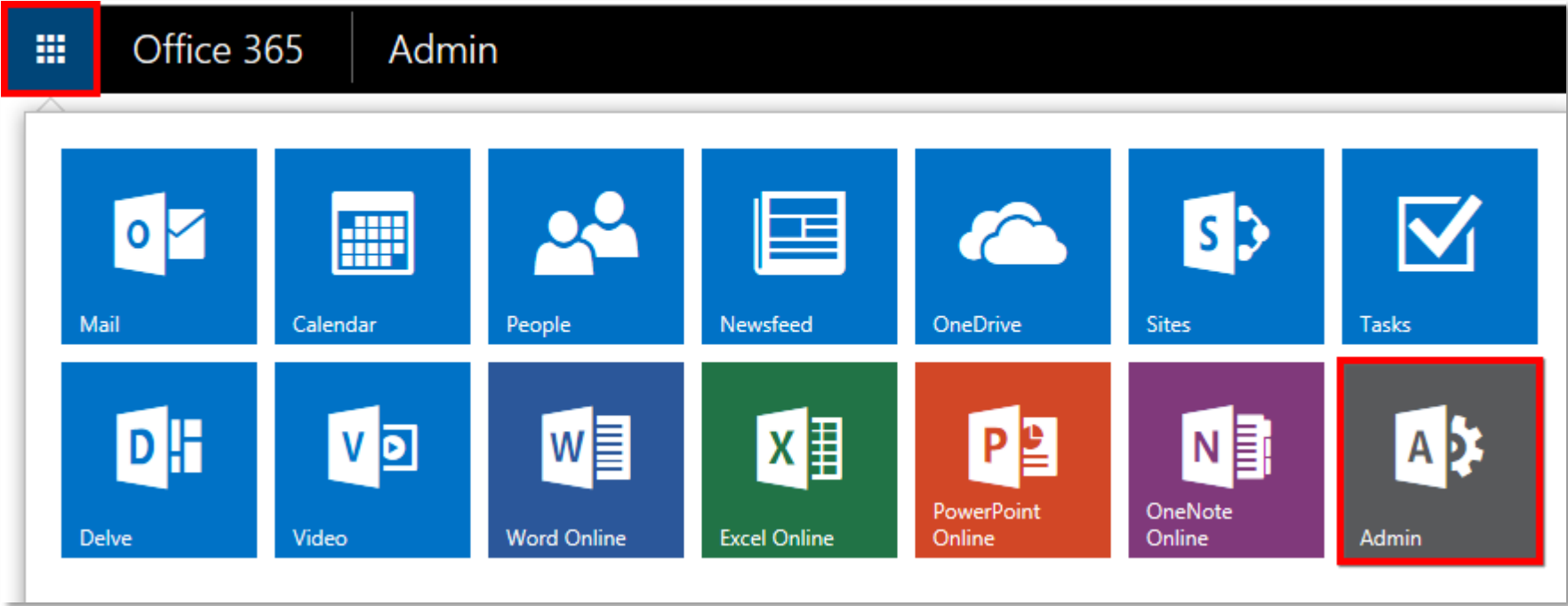
To make this happen you need to create 3 things in your Office 365 portal:

1. A “Send” Connector. This redirects each message to the Exclaimer Cloud where the signature is added before it is delivered to the recipient(s).
2. A “Receive” Connector. When the Exclaimer Cloud has added the signature, it returns the message back to Office 365 through the Receive Connector.
3. A “Transport Rule”. This will ensure that each message doesn’t get sent more than once to the Exclaimer Cloud.

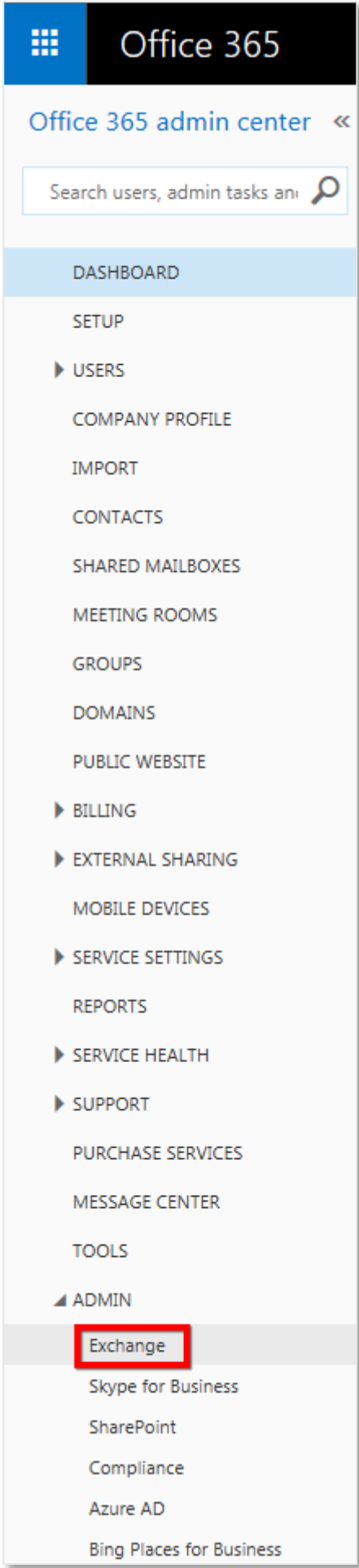
Follow the step-by-step instructions below or watch our comprehensive video guide, which can be accessed [here](#).

Step 1: Go to the Exchange mail flow section of the Office 365 portal

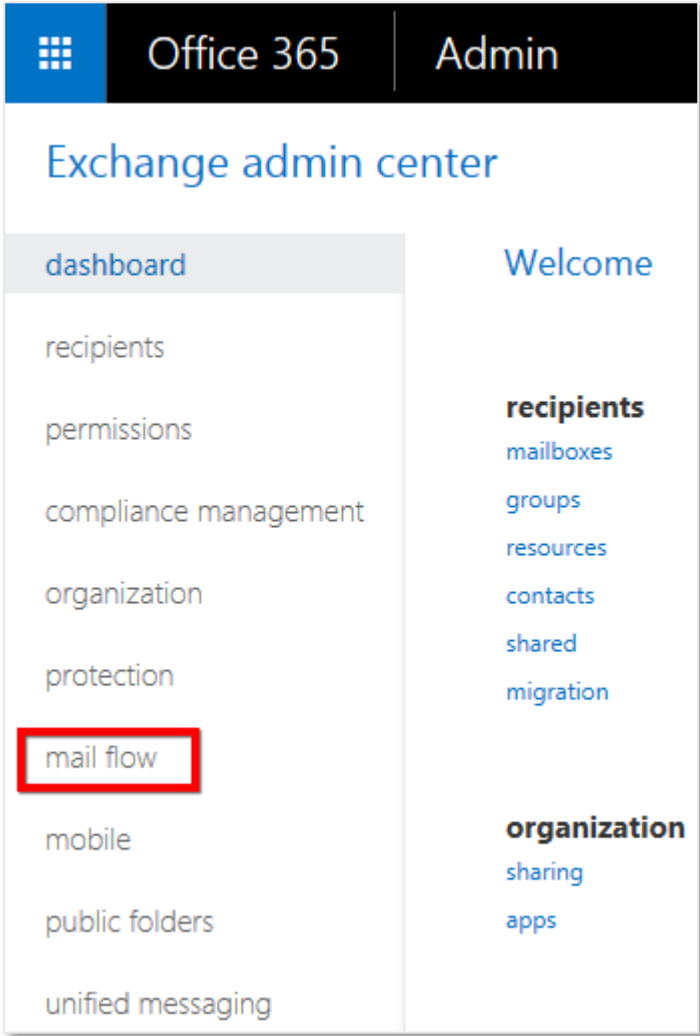
- a) Sign into your organization’s Office 365 tenancy via the [Office 365 portal](#) as an Administrator.
- b) At the Home screen, click the icon at the top left of the screen and select the ‘**Admin**’ option from the menu that appears:



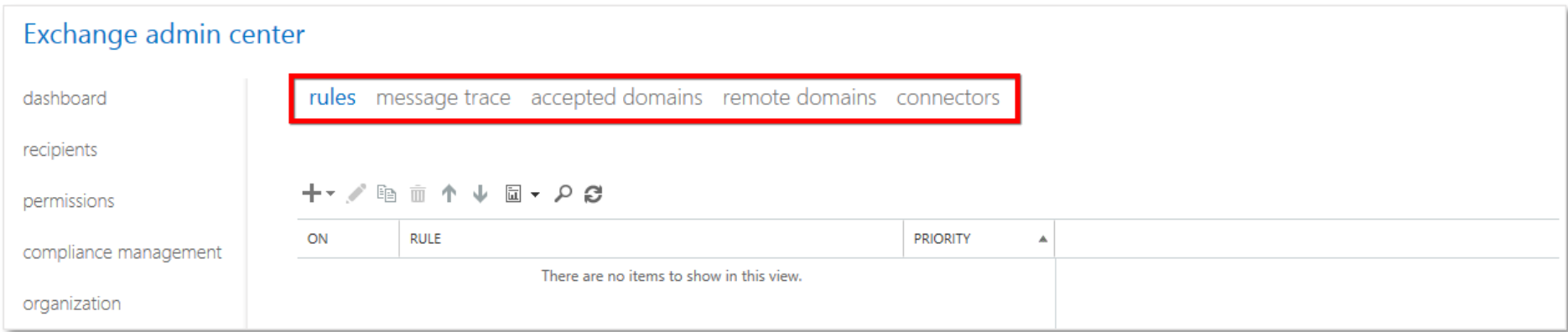
- c) You will now arrive at the ‘**Office 365 admin center**’ page. From the menu on the left, go to the ‘**ADMIN**’ option and select ‘**Exchange**’:



d) The ‘Exchange admin center’ page will open. From the menu on the left, select the ‘mail flow’ option:

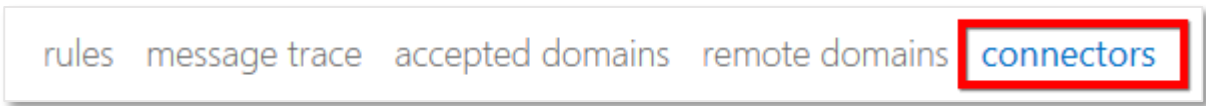


e) You will now arrive at the ‘mail flow’ page, with a row of options along the top:

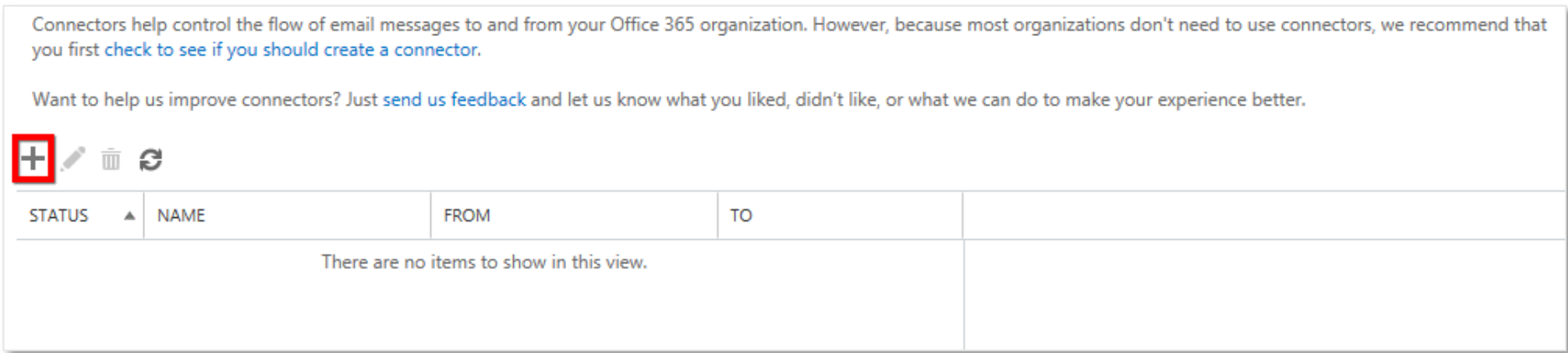


Step 2: Set up the ‘Send’ Connector

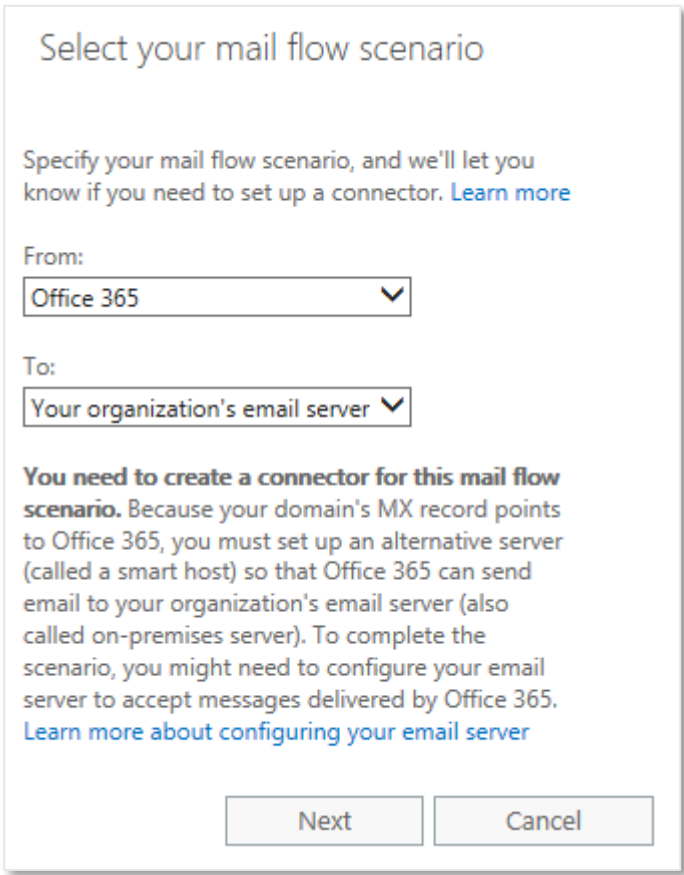
a) At the ‘mail flow’ page Select the ‘Connectors’ option:



b) The screen will change to show the Connectors list. Click the ‘+’ icon to start creating the Send Connector:



c) The Connector creator will appear. On the ‘Select your mail flow scenario’ page set the ‘From’ dropdown to ‘Office 365’ and the ‘To’ dropdown to ‘Your organization’s email server’ and then click ‘Next’:



d) On the next page give your Send Connector a descriptive name and, optionally, a more detailed description. Ensure that you leave the two checkboxes enabled, then click ‘Next’:

New connector

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

*Name:

Send to Exclaimer Cloud

Description:

Connector for my Office 365 signatures

What do you want to do after connector is saved?

☒ Turn it on

☒ Retain internal Exchange email headers (recommended)

Next

Cancel

e) On the next page select the radio option ‘**Only when I have a transport rule set up that redirects messages to this connector**’, then click ‘**Next**’ (you will set up the transport rule in Step 4):

New connector

When do you want to use this connector?

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

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

☐ Only when email messages are sent to these domains

+

-

Back

Next

Cancel

f) Next you will be asked how to route messages. Click the ‘+’ icon to add a smart host to this list:

New connector

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. [Learn more](#)

+

-

Back

Next

Cancel

g) In the ‘**add smart host**’ box that pops up, enter **smtp.eu1.exclaimer.net** then click ‘**Save**’:

add smart host

Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.
Example: myhost.contoso.com or 192.168.3.2

smtp.eu1.exclaimer.net

Save

Cancel

h) You will be returned to the smart host list with your entry now present. Click **‘Next’**:

New connector

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. [Learn more](#)

+-

smtp.eu1.exclaimer.net

Back

Next

Cancel

i) The next page relates to the security of the connection. Leave the **‘Always use Transport Layer Security (TLS)’** option checked, and ensure that the **‘Issued by a trusted certificate authority (CA)’** radio option is selected. Click **‘Next’**:

New connector

How should Office 365 connect to your email server?

☒ 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:
Example: contoso.com or *.contoso.com

Back

Next

Cancel

j) The confirmation page will appear. Confirm that the settings are correct then click **‘Next’**:

New connector

Confirm your settings

Before we validate this connector for you, make sure these are the settings you want to configure.

Mail flow scenario

From: Office 365

To: Your organization's email server

Name

Send to Exclaimer Cloud

Description

Connector for my Office 365 signatures

Status

Turn it on after saving

When to use the connector

Use only when I have a transport rule set up that redirects messages to this connector.

Routing method

Route email messages through these smart hosts: smtp.eu1.exclaimer.net

Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server certificate is issued by a trusted certificate authority (CA).

Back

Next

Cancel

k) The connector validation page will appear, which requires you to send a test message. Click the **‘+’** icon to specify an email recipient for the test message:

New connector

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

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

+

−

Back

Validate

Cancel

- l) In the **‘add email’** box that pops up, enter the email address of the recipient of your test mail (note that this email address must not belong to an Office 365 mailbox), then click **‘OK’**:

add email

Send the test email to this address:

karen@greenorg.net

OK

Cancel

- m) You will be returned to the connector validation page with your email entry now present. Click **‘Validate’**:

New connector

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

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

+

−

karen@greenorg.net

Back

Validate

Cancel

- n) The validation process will start:

New connector

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

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

+

−

karen@gr

Step 1 of 3: Validating smart host...

Click 'Stop' to cancel the operation. Stopping the operation won't undo the changes already applied.

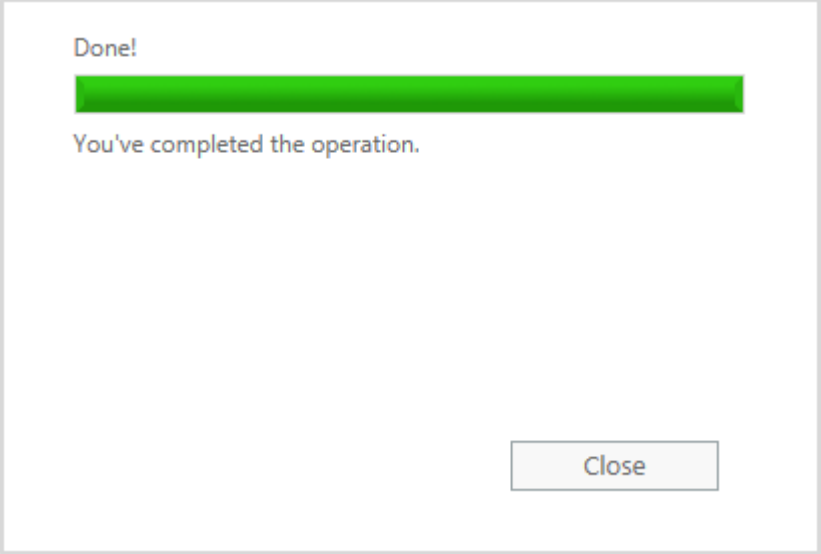
stop

Back

Validate

Cancel

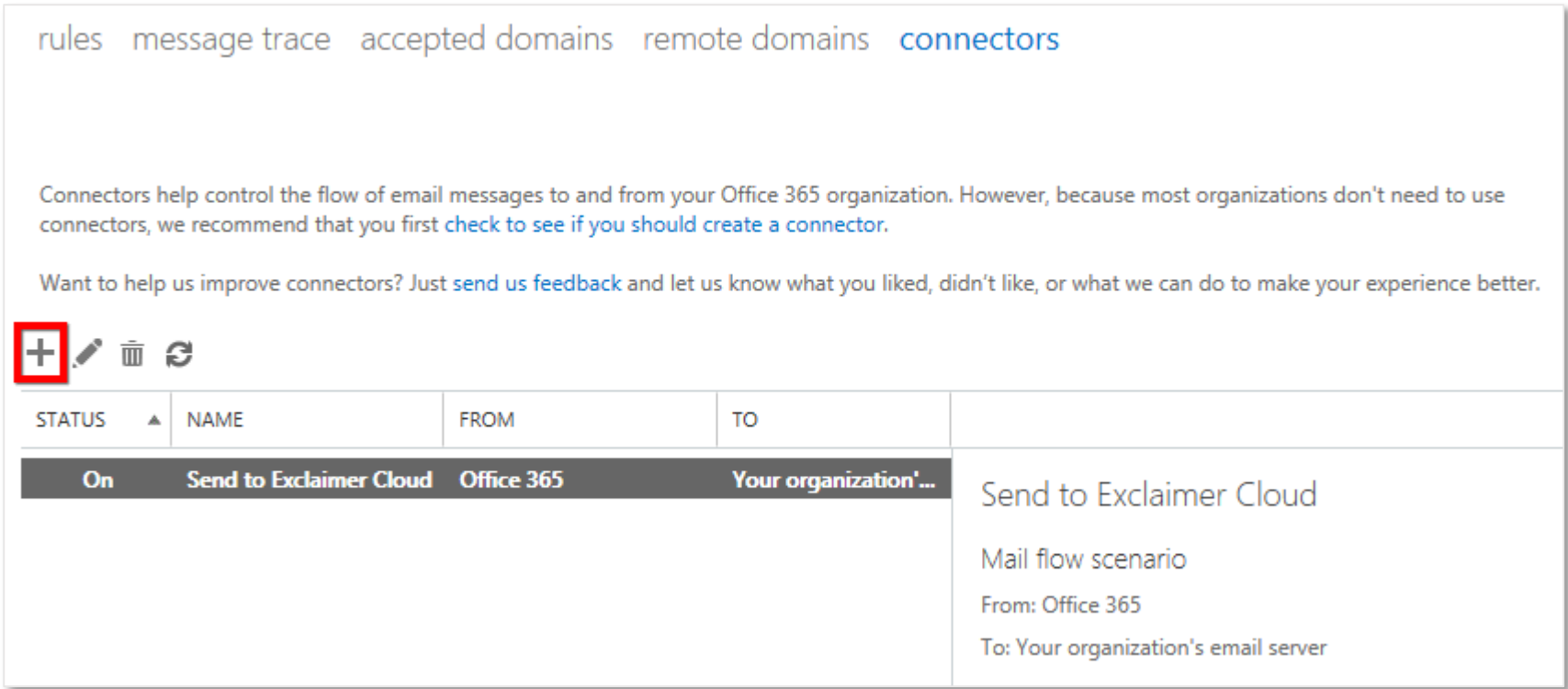
o) When it has finished, click **‘Close’**, then click **‘Save’** to complete the creation of the Send Connector:



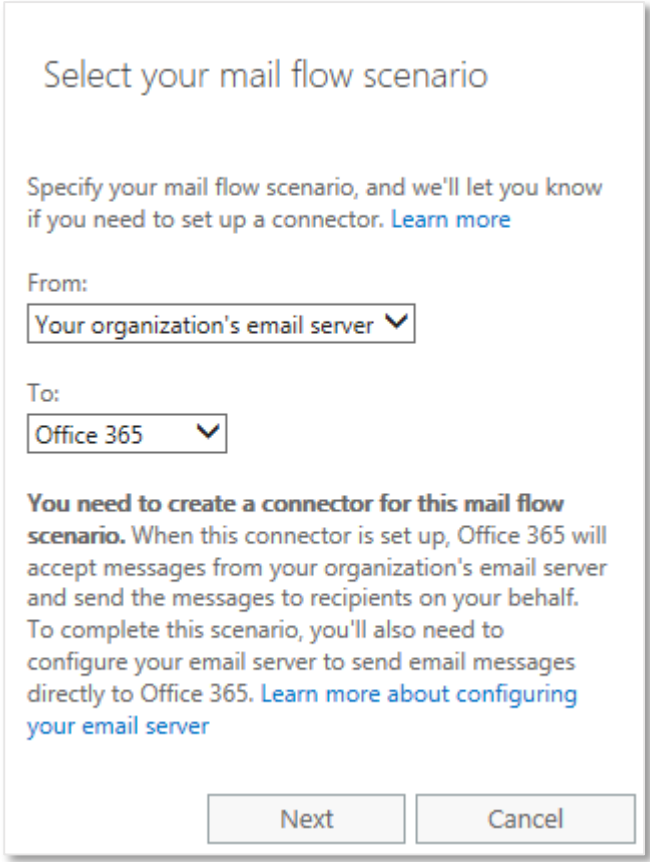
NOTE: Microsoft advise that a newly created Connector may take as long as 15 minutes to become operational.

Step 3: Set up the ‘Receive’ Connector

a) Having completed the setup of the Send Connector you should now be back at the **‘Connectors’** section of the **‘mail flow’** page. Click the **‘+’** icon to start creating the Receive Connector:



b) The Connector creator will appear. On the **‘Select your mail flow scenario’** page set the **‘From’** dropdown to **‘Your organization’s email server’** and the **‘To’** dropdown to **‘Office 365’** and then click **‘Next’**:



c) On the next page give your Receive Connector a descriptive name and, optionally, a more detailed description. Ensure that the **‘Turn it on’** option is checked and that the **‘Retain internal Exchange email headers (recommended)’** is unchecked, then click **‘Next’**:

New connector

This connector lets Office 365 accept email messages from your organization's email server (also called an on-premises server).

*Name:
Receive from Exclaimer Cloud

Description:
Connector to receive messages after signatures have been applied

What do you want to do after connector is saved?
☒ Turn it on
☐ Retain internal Exchange email headers (recommended)

Next

Cancel

d) On the next page select the radio option ‘By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches this domain name (recommended)’. In the field below, enter **smtp.exclaimer.net** then click ‘Next’:

New connector

How should Office 365 identify email from your email server?

☒ By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches this domain name (recommended)
smtp.exclaimer.net

☐ By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization
+ ✎ -

Office 365 will only accept messages through this connector if the sender domain is configured as an accepted domain for your Office 365 organization. [Learn more](#)

Back

Next

Cancel

e) The confirmation page will appear. Confirm that the settings are correct then click ‘Save’:

New connector

Confirm your settings
Before saving, make sure these are the settings you want to configure.

Mail flow scenario
From: Your organization's email server
To: Office 365

Name
Receive from Exclaimer Cloud

Description
Connector to receive messages after signatures have been applied

Status
Turn it on after saving

How to identify email sent from your email server
Identify email coming from your email server by verifying the subject name on the connecting TLS certificate matches this domain: smtp.exclaimer.net, and the sender domain is an accepted domain for your organization.

Back

Save

Cancel

- f) Having completed the setup of the Receive Connector you should now be back at the ‘Connectors’ section of the ‘mail flow’ page with your Send and Receive connectors both listed:

[rules](#) [message trace](#) [accepted domains](#) [remote domains](#) [connectors](#)

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first [check to see if you should create a connector](#).

Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

+

STATUS	NAME	FROM	TO	
On	Receive from Exclaimer Cloud	Your organization's email server	Office 365	Receive from Exclaimer Cloud
On	Send to Exclaimer Cloud	Office 365	Your organization's email server	Mail flow scenario
				From: Your organization's email server
				To: Office 365
				Description
				Connector to receive messages after signatures have been applied

NOTE: Microsoft advise that a newly created Connector may take as long as 15 minutes to become operational.

Step 4: Create the Transport Rule

- a) Having completed the setup of the Receive Connector you should now be back at the ‘Connectors’ section of the ‘mail flow’ page. From the row of options along the top, select ‘rules’:

[rules](#) [message trace](#) [accepted domains](#) [remote domains](#) [connectors](#)

- b) The screen will change to show the Rules list. Click the ‘+’ icon and select ‘Create a new rule...’ from the dropdown menu:

[rules](#) [message trace](#) [accepted domains](#) [remote domains](#) [connectors](#)

+

Create a new rule...

Apply rights protection to 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...

There are no items to show in this view.

- c) The Rule creator will appear. Give your rule a descriptive name and then click the ‘More options...’ hyperlink:

new rule

Name:

Identify messages to send to Exclaimer Cloud

X

*Apply this rule if...

Select one

*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...

Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. [Learn more](#)

Save

Cancel

d) From the ‘Apply this rule if...’ dropdown, select ‘The sender...’ and then ‘is external/internal’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

Select one

The sender...

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

☒ Audit this rule with severity level:

Not specified

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

Save

Cancel

e) In the ‘select sender location’ box that pops up, ensure that ‘Inside the organization’ is selected, then click ‘OK’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

*Select one...

add condition

*Do the following...

Select one

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

Save

Cancel

select sender location

Inside the organization

OK

Cancel

f) From the ‘Do the following...’ dropdown, select ‘Redirect the message to...’ and then ‘the following connector’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

[Inside the organization](#)

add condition

*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...

Notify the recipient with a message...

these recipients

hosted quarantine

the following connector

☐ Test with Policy Tips

☐ Test without Policy Tips

Save

Cancel

g) In the ‘select connector’ box that pops up, ensure that the Send connector that you created in Step 2 is selected, then click ‘OK’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

[Inside the organization](#)

add condition

*Do the following...

Use the following connector...

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

Save

Cancel

select connector

Connector:

Send to Exclaimer Cloud

OK

Cancel

h) Now click the ‘add exception’ button:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

[Inside the organization](#)

add condition

*Do the following...

Use the following connector...

[Send to Exclaimer Cloud](#)

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

Save

Cancel

i) From the ‘Except if...’ dropdown, select ‘A message header...’ and then ‘matches these text patterns’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

[Inside the organization](#)

add condition

*Do the following...

Use the following connector...

[Send to Exclaimer Cloud](#)

add action

Except 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...

☐ Test without Policy Tips

includes any of these words

matches these text patterns

Save

Cancel

j) Now click the ‘Enter text...’ hyperlink:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

[Inside the organization](#)

add condition

*Do the following...

Use the following connector...

[Send to Exclaimer Cloud](#)

add action

Except if...

✕ A message header matches...

*Enter text...

header matches [*Enter text patterns...](#)

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

Save

Cancel

k) In the ‘specify header name’ box that pops up enter **X-ExclaimerHostedSignatures-MessageProcessed** then click ‘OK’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

[Inside the organization](#)

add condition

*Do the following...

Use the following connector...

add action

Except if...

✕ A message header matches...

specify header name

X-ExclaimerHostedSignatures-MessageProcessed

OK

Cancel

header matches [*Enter text patterns...](#)

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

Save

Cancel

l) Now click the ‘Enter text patterns...’ hyperlink:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

add condition

Inside the organization

*Do the following...

Use the following connector...

add action

Send to Exclaimer Cloud

Except if...

✕

A message header matches...

add exception

'X-ExclaimerHostedSignatures-MessageProcessed'
header matches

Enter text patterns...

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

Save

Cancel

m) In the ‘specify words or phrases’ box that pops up, enter true (in lower case), click the ‘+’ icon to add the phrase to the list, and then click the ‘OK’ button:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

add condition

Inside the organization

*Do the following...

Use the following connect

add action

Send to Exclaimer Cloud

Except if...

✕

A message header matche

add exception

'X-ExclaimerHostedSignatures-MessageProcessed'
header matches

Enter text patterns...

Properties of this rule:

☒ Audit this rule with sev

Not specified

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

Save

Cancel

specify words or phrases

true

+

OK

Cancel

n) Now click the ‘add exception’ button again and from the ‘or...’ dropdown, select ‘The sender...’ and then ‘address matches any of these text patterns’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

add condition

Inside the organization

*Do the following...

Use the following connector...

add action

Send to Exclaimer Cloud

Except if...

✖ A message header matches...

'X-ExclaimerHostedSignatures-MessageProcessed'
header matches 'true'

or

✖ 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...

☐ Test without Policy Tips

☐ Activate this rule on the following date:

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

o) In the ‘specify words or phrases’ box that pops up, enter <>, click the ‘+’ icon to add the phrase to the list, and then click the ‘OK’ button:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

add condition

Inside the organization

*Do the following...

Use the following connect

add action

Send to Exclaimer Cloud

Except if...

✖ A message header matche

atures-MessageProcessed'

or

✖ The sender address match

add exception

Properties of this rule:

☒ Audit this rule with sev

Not specified

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

Save

Cancel

specify words or phrases

<>

+

OK

Cancel

p) Now click the ‘add exception’ button a third time and from the second ‘or...’ dropdown, select ‘The message properties...’ and then ‘include the message type’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

add condition

Inside the organization

*Do the following...

Use the following connector...

add action

Send to Exclaimer Cloud

Except if...

✕ A message header matches...

'X-ExclaimerHostedSignatures-MessageProcessed' header matches 'true'

or

✕ The sender address matches...

'<>'

or

✕ 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...

include the message type

include this classification

don't include any classification

include an SCL greater than or equal to

include the importance level

Save

Cancel

q) In the ‘select message type’ box that pops up ensure that ‘Calendaring’ is selected, then click ‘OK’:

new rule

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

The sender is located...

add condition

Inside the organization

*Do the following...

Use the following connector...

add action

Send to Exclaimer Cloud

Except if...

✕ A message header matches...

'X-ExclaimerHostedSignatures-MessageProcessed' header matches 'true'

or

✕ The sender address matches...

'<>'

or

✕ The message type is...

*Select one...

add exception

Properties of this rule:

☒ Audit this rule with severity level:

Not specified

Save

Cancel

select message type

Calendaring

OK

Cancel

r) Click the ‘Save’ button to complete creation of the rule.

NOTE: Microsoft advise that a newly created transport rule may take as long as 1 hour to become operational.

Step 5 (OPTIONAL): Limit the number of users whose messages are sent to the Exclaimer Cloud

You may want to test Exclaimer Cloud Signatures for Office 365 using a restricted number of users before rolling it out more widely. The simplest way to do this is by using a Distribution Group populated only with the users whose messages you want to send to the Exclaimer Cloud.

- a) From the menu on the left of the Exchange admin center, click ‘recipients’ and select ‘groups’ from the row of options along the top. Click the ‘+’ icon to create your group, and select ‘Distribution group’ from the dropdown menu:

Identify messages to send to Exclaimer Cloud

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

×

The sender is located...

▼

Inside the organization

and

×

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...

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

×

The message type is...

▼

or

×

A message header matches...

▼

'X-ExclaimerHostedSignatures-MessageProcessed'
header matches 'true'

add exception

Save

Cancel

f) The Group selector will appear. Highlight the Group that you created in point b) above, then click the ‘add ->’ button:

🔍 ↺ ...

DISPLAY NAME

EMAIL ADDRESS

Exclaimer Cloud Signatures Group

signatures@exclaimer.onmicrosoft.com

My Office 365 Administrator

admin@exclaimer.onmicrosoft.com

1 selected of 2 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.

add ->

Exclaimer Cloud Signatures Group[remove];

check names

OK

Cancel

g) Confirm that your changes have taken effect, then click the ‘Save’ button to complete the modifications to the rule:

Identify messages to send to Exclaimer Cloud

Name:

Identify messages to send to Exclaimer Cloud

*Apply this rule if...

×

The sender is located...

▼

Inside the organization

and

×

The sender is a member of...

▼

'Exclaimer Cloud Signatures Group'

add condition

*Do the following...

Use the following connector...

▼

Send to Exclaimer Cloud

add action

Except if...

×

The sender address matches...

▼

'<>'

or

×

The message type is...

▼

Calendaring

or

×

A message header matches...

▼

'X-ExclaimerHostedSignatures-MessageProcessed'
header matches 'true'

add exception

Save

Cancel

NOTE: Microsoft advise that changes to a transport rule may take as long as 1 hour to become operational.