



DataMotion Secure Message Center Integration Guide for Microsoft 365

February 19, 2024
Part # 050013-06

Copyright © 2008 - 2024, DataMotion, Inc. (“DataMotion”). ALL RIGHTS RESERVED.
Your right to print, copy, reproduce, publish or distribute this document or parts of this document is limited by copyright law.

DataMotion® is a registered trademark of DataMotion, Inc. All other brand and product names are trademarks or registered trademarks of their respective companies.

The information contained in this document is subject to change without notice. THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. IN NO EVENT SHALL DATAMOTION BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING FROM ANY ERROR IN THIS DOCUMENT, INCLUDING WITHOUT LIMITATION ANY LOSS OR INTERRUPTION OF BUSINESS, PROFITS, USE, OR DATA.

DataMotion Secure Message Center Integration Guide for Microsoft 365 v6

Publication Date: February 19, 2024

Printed in the United States of America.

DataMotion, Inc. Confidential and Proprietary Information.

Published By:

DataMotion, Inc.
200 Park Ave.
Florham Park, NJ 07932
USA

1 800-672-7233 or +1 973-455-1245

<http://www.datamotion.com/>

TABLE OF CONTENTS

ABOUT THIS PUBLICATION	7
ABOUT THE DATAMOTION SECURE MESSAGE CENTER	7
INTENDED AUDIENCE	7
HOW TO USE THIS PUBLICATION	8
RELATED INFORMATION	8
DataMotion Documentation	8
1 INTRODUCTION	9
DATAMOTION SECURE MESSAGE CENTER FOR MICROSOFT 365.....	9
Important Note About the Secure Tag	10
2 OVERVIEW OF THE SETUP	11
SETUP PROCEDURE (SUMMARY)	11

3 INTEGRATE DATAMOTION SMC WITH MICROSOFT 365

12

REVIEW THE REQUIREMENTS 12

Connector Domain Requirements 12

CREATE A CONNECTOR TO ROUTE MESSAGES TO DATAMOTION 13

USE MICROSOFT EXCHANGE TO CREATE A RULE WITH A SECURE TAG 22

SEND A SECURE MESSAGE (TO CONFIRM OPERATION) 30

CREATING A CONNECTOR AND AN ASSOCIATING RULE FOR INBOUND SECURE MESSAGES (OPTIONAL)..... 31

Connector IP Address Requirements 31

Creating a Connector for Internal Secure Communications..... 31

Creating the Mail Rule for Internal Secure Communications..... 37

Send a Secure Message Internally to Ensure Personnel Receive the Appropriate Banner 47

REVISION HISTORY

This section summarizes significant changes, corrections, and additions to the document. The history appears in chronological order with the most recent changes listed first.

Version 6

Updates made throughout to Microsoft 365 terminology from Office 365.

Chapter 3: *Integrate DataMotion SMC with Microsoft 365*

- Changed images for the Microsoft 365 interface and associated instructions throughout the chapter.
- Added multiple new sections for performing internal secure communications.

Version 5

Chapter 3: *Integrate DataMotion SMC with Microsoft 365*

- (Section Removed.)
 - » Changed the SPF record in this section to match the new IP address.

Version 4

Chapter 3: *Integrate DataMotion SMC with Microsoft 365*

- *Review the Requirements* (on page 12)
 - » Removed references to the Office 365 versions that include DLP settings as these no longer apply to the instructions within this document.
- *Use DLP to Create Transport Rule with a Secure Tag*
 - » This section has been removed from the document as it is no longer supported.
- *Create a Connector to Route Messages to DataMotion* (on page 13)
 - » Made significant updates to the instructions to create a connector as the workflow in Office 365 to do so has changed.
 - » Many of the screenshots were also updated to reflect these changes.

Version 3

Chapter 1: *Introduction*

- *Important Note About the Secure Tag* (on page 10)

- » This is a new section that has been included before the instructions begin to inform the reader that the [Secure] tag is just an example and does not have to be the only form the tag can take.

Version 2

Chapter 3: *Integrate DataMotion SMC with Microsoft 365*

-
- *Use Microsoft Exchange to Create a Rule with a Secure Tag* (on page 21)
- This is a new section that describes setting up Office 365 plans that do not have Data Loss Prevention as an included feature.

Version 1

Initial version of this document.

About This Publication

ABOUT THE DATAMOTION SECURE MESSAGE CENTER

This publication describes how to integrate the DataMotion Secure Message Center (commonly referred to as the DataMotion SMC for short) for use with Microsoft 365.

The DataMotion SMC provides easy-to-use secure data exchange for protecting vital information flowing between you, your business partners, and your clients.

DataMotion SMC protects sensitive data with military-grade encryption, and it allows users to send secure messages and files using one click, with built-in tracking of all messages and files sent, received, and opened. The DataMotion SMC can be integrated with popular email clients such as Microsoft Outlook, and it is intuitive for users of all levels of skill, so it can be up and running in minutes with no outside IT support.

Providing effortless secure communications from email clients and direct delivery to the recipient's inbox, plus the ability to transfer large files easily from desktop clients or mobile devices, DataMotion Secure Message Center offers unsurpassed capability, flexibility, and user experience.

INTENDED AUDIENCE

This publication is intended for a technical audience, including system administrators and system integrators.

Additional technical documentation, as well as user documentation, is also available from DataMotion. See [DataMotion Documentation](#) (on page 8).

HOW TO USE THIS PUBLICATION

The content is organized as follows:

About This Publication.

Provides an overview of the content of this publication and how to use the publication.

Chapter 1) Introduction

Describes DataMotion Secure Message Center for Microsoft 365.

Chapter 2) Overview of the Setup

Provides a synopsis of the setup procedures.

Chapter 3) Integrate DataMotion SMC with Microsoft 365

Provides step-by-step instructions on how to set up Microsoft 365 for use with DataMotion Secure Message Center.

Chapter Error! Reference source not found.) Error! Reference source not found.

Provides additional technical information for using DataMotion Secure Message Center with Microsoft 365.

RELATED INFORMATION

DATAMOTION DOCUMENTATION

- *DataMotion Secure Message Center User Guide* (part # 050004)
Provides instructions for using the products.
- *DataMotion Secure Message Center Administration Guide* (part # 050006)
Documents the system installation, maintenance, and administration tools for administrators and integrators.

Additional documentation is available on many other topics. Please contact DataMotion Support for more information.

1

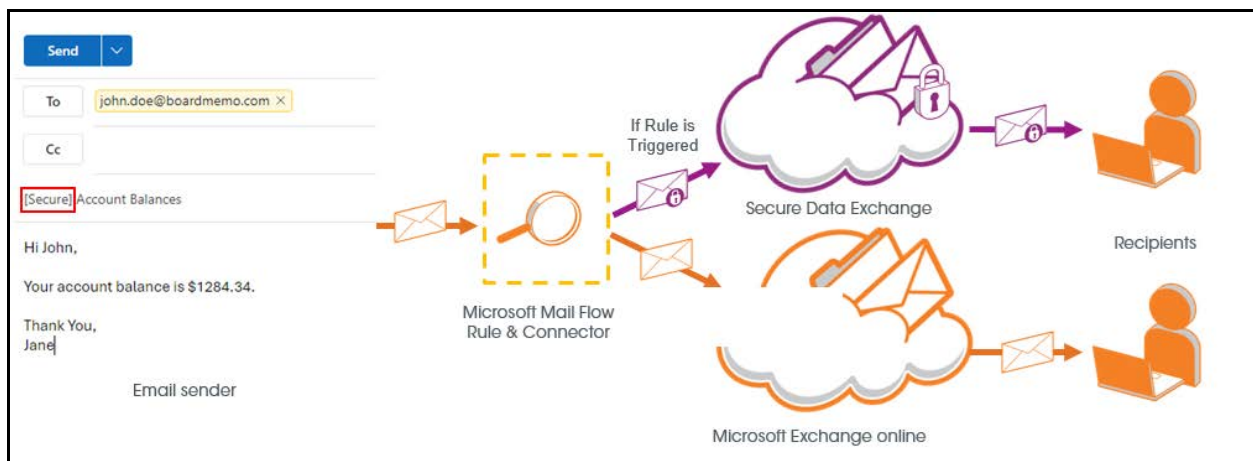
Introduction

DATAMOTION SECURE MESSAGE CENTER FOR MICROSOFT 365

DataMotion Secure Message Center enables businesses to protect sensitive data and maintain compliance with privacy and security regulations while taking advantage of cloud-based email solutions with all their benefits.

With DataMotion Secure Message Center for Microsoft 365, users are able to send secure messages from their email clients of choice by simply inserting a predefined word or phrase in the subject line and clicking send. DataMotion Secure Message Center for Microsoft 365 is easy to use because it integrates with applications, mobile devices and systems already in use without the need to install special applications or exchange encryption keys.

The following diagram illustrates how easy it is to integrate DataMotion Secure Message Center with Microsoft 365.



Going from left to right in the diagram (from Email Sender to Recipients): Simply by adding a "[Secure]" tag in the subject line of the email, the sender identifies the email as a secure message. When the email is sent, the Mail Flow Rule of your Exchange server (created in the

Use Microsoft Exchange to Create a Rule with a Secure Tag section) will route the message to a connector (created in the Create a Connector to Route Messages to DataMotion section) which sends the message securely based on presence of the tag in the subject line.

Using Transport Layer Security (TLS), which is an encryption protocol that provides secure communication over the Internet, Microsoft will route sensitive email to the DataMotion Secure Message Center host, which then delivers it securely to recipients.

This guide provides easy to follow, step-by-step instructions describing how to integrate DataMotion Secure Message Center into Microsoft 365 cloud-based email environments.

IMPORTANT NOTE ABOUT THE SECURE TAG

Throughout this document the [Secure] tag that is used should ideally be added to the beginning of the Subject line when constructing messages.

2

Overview of the Setup

DataMotion Secure Message Center for Microsoft 365 is easily integrated into the Microsoft 365 environment. It uses Exchange Mail Flow Rules and Connectors to route email based on the presence of a “[Secure]” tag.

Once the DataMotion Secure Message Center is integrated with Microsoft 365, no additional applications or setup is required by users.

SETUP PROCEDURE (SUMMARY)

During the setup procedures, you will do the following:

1. ***Review the Requirements*** (on page 12):
Make sure you have met the requirements before performing the procedures.
2. ***Create a Connector to Route Messages to DataMotion*** (on page 13):
Create an outbound connector to set up email routing to the DataMotion Secure Message Center gateway. This enables secure messages to be processed properly by the DataMotion SaaS.
3. ***Use Microsoft Exchange to Create a Rule with a Secure Tag*** (on page 21)
Create a Microsoft Exchange rule to scan for a subject line tag of “[Secure]”.
4. ***Send a Secure Message (to Confirm Operation)*** (on page 30):
Confirm the operation by creating and sending a secure message.

The setup procedures are designed to be performed in sequence, unless otherwise noted, and later procedures assume that all prior steps have been performed.

3

Integrate DataMotion SMC with Microsoft 365

The information detailed throughout this chapter describes how to integrate DataMotion Secure Message Center with Microsoft 365 for a seamless and secure experience. (See the [Overview of the Setup](#) for a synopsis of the procedures.)

REVIEW THE REQUIREMENTS

You must meet the following requirements to perform the DataMotion Secure Message Center setup for Microsoft 365:

1. Your Microsoft 365 setup must be complete, and Microsoft 365 must be able to send and receive messages.
2. You must have Microsoft 365 administrative rights (in particular an Exchange Administrator role) to perform the setup procedures in this guide.
3. You must have a DataMotion Secure Message Center account that has been provisioned and is ready to send secure messages.

CONNECTOR DOMAIN REQUIREMENTS

When creating the connector (highlighted in the steps below) you will be required to enter a domain. The domain that should be entered will vary depending on geographical region and the appropriate domains are listed below:

- US region: **scpusv7.datamotion.com**
- CA region: **scpcav7.datamotion.ca**

NOTE: It is imperative that you enter the correct domain for your region when setting up the connector. If you are not sure of the domain you should use please contact DataMotion Support at support@datamotion.com for assistance.

CREATE A CONNECTOR TO ROUTE MESSAGES TO DATAMOTION

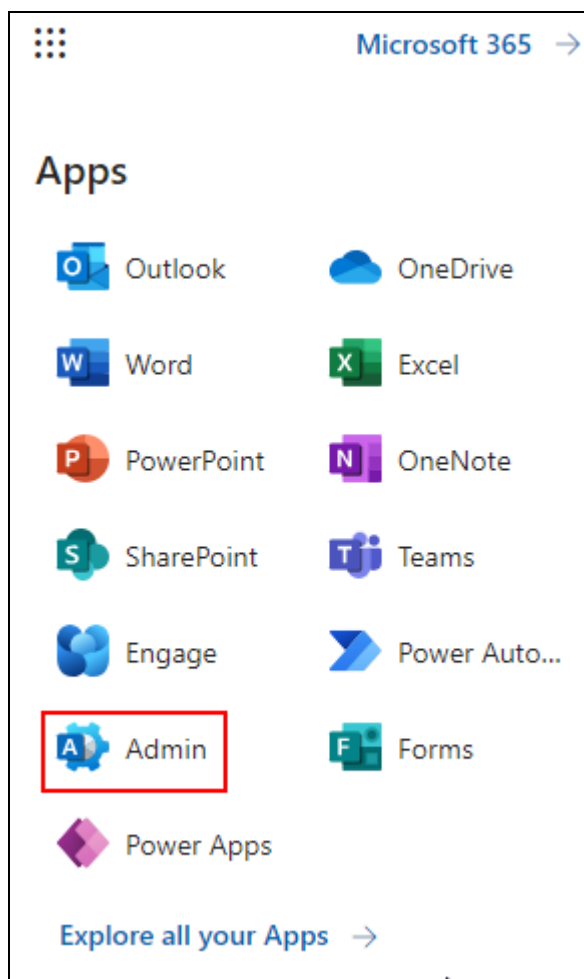
This procedure describes how to set up email routing to the DataMotion Secure Message Center gateway. This enables secure messages to be processed properly.

In the Microsoft 365 administration portal, you will use the Exchange Administration Center to add a Connector with TLS applied. A Connector is used to control the flow of outbound email messages to a receiving server, which in this case is the DataMotion Secure Message Center smart host. (A smart host is a server that redirects outbound mail.) TLS ensures secure, encrypted routing to DataMotion. These steps assume that you are logged into Microsoft 365.

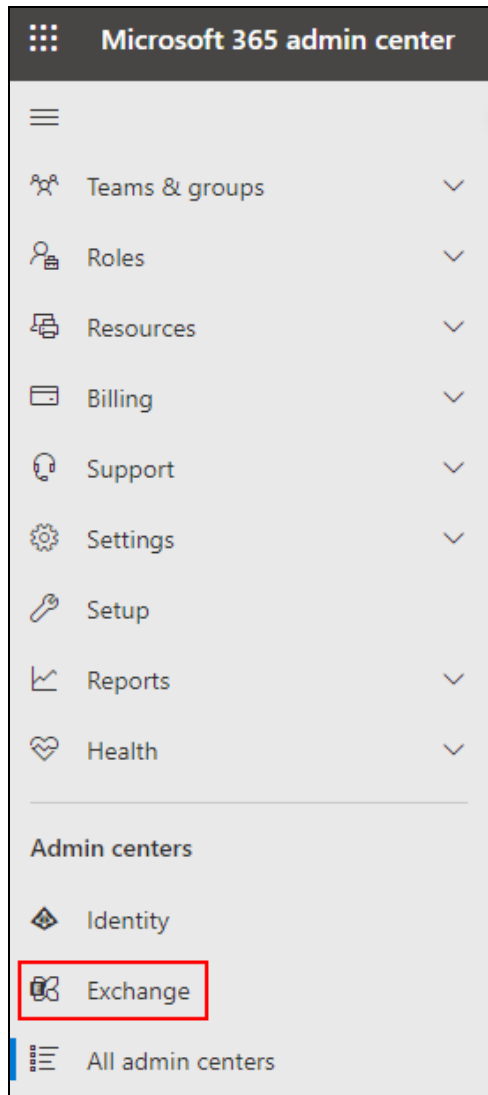
1. Open the Apps menu by clicking the 3x3 dots icon (typically looks like the image below).



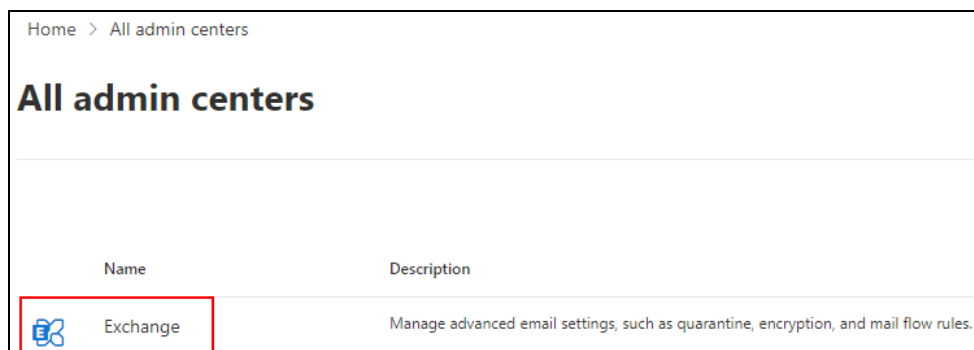
2. Select **Admin** (your available Apps and their order may differ).



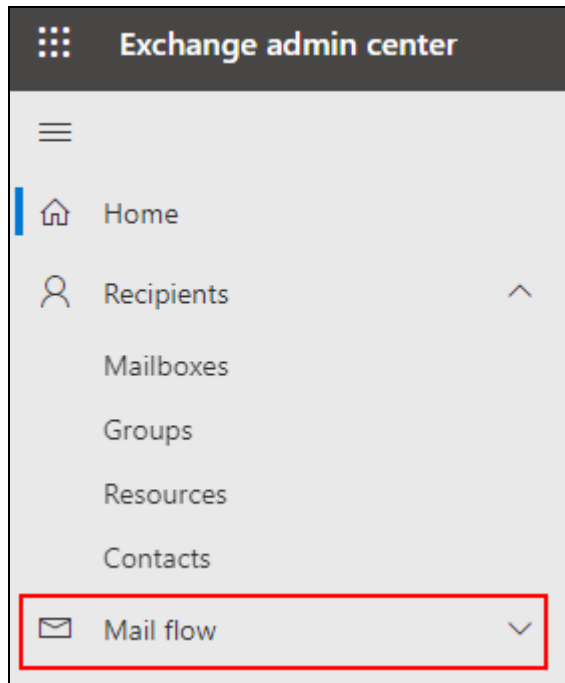
3. Under the **Microsoft 365 admin center** pull out scroll down to the **Admin centers** section, and select **Exchange**.



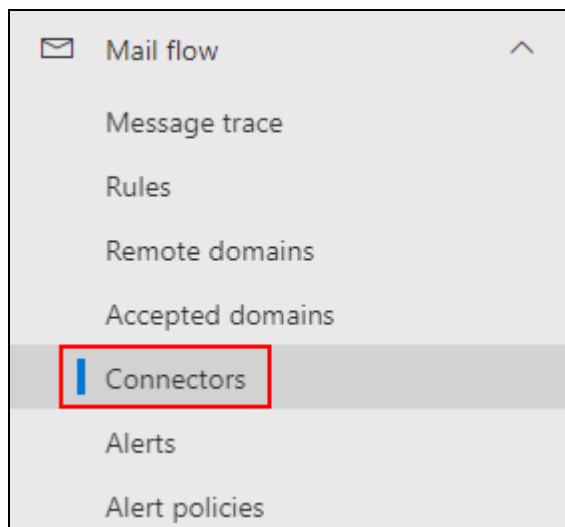
- » If Exchange does not appear initially, you can select **All admin centers** and then Exchange.



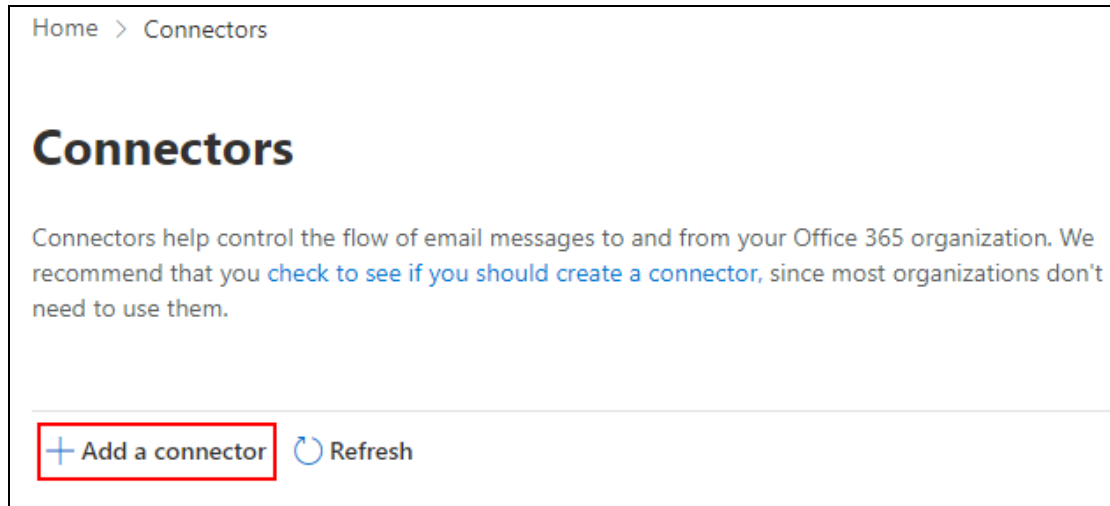
4. Once **Exchange admin center** opens, click the **Mail flow** section on the left side of the screen.



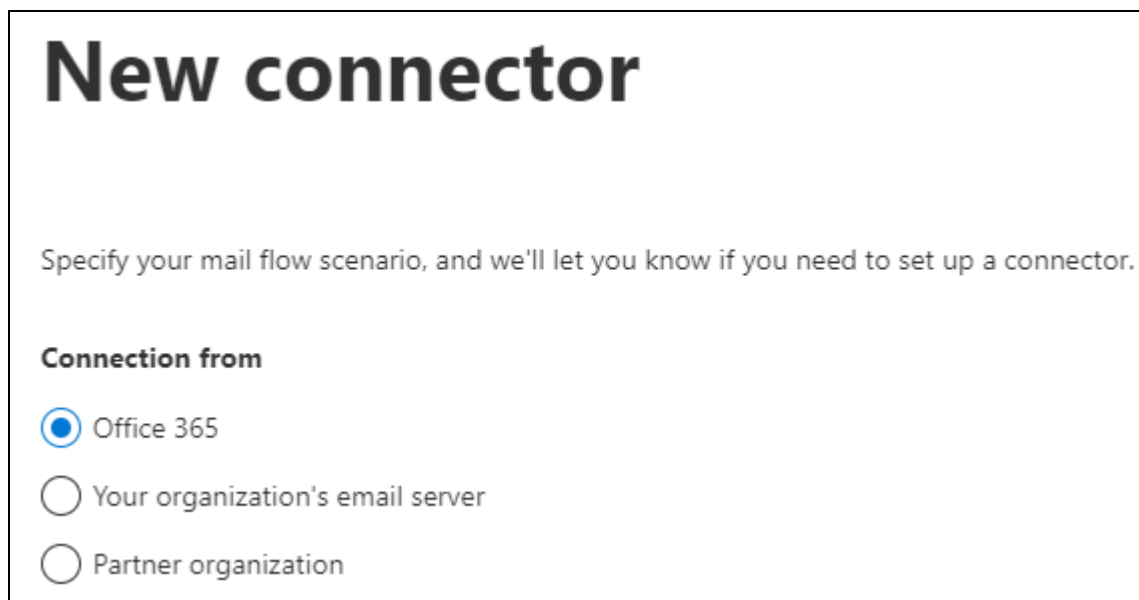
5. Click **Connectors**.



6. On the **Connectors** screen, click the **Add a connector** button to create a new connector.



7. The **New connector** screen provides three options for the **Connection from**. For these instructions we will use **Office 365**.



8. Select **Partner organization** for the **Connection to**.
9. Click **Next**.

Connection to

☐ Your organization's email server

☒ Partner organization ①

② **Next**

10. Enter a **Name** for the connector.
11. Enter a **Description** about what action the connector performs (see screenshot example).
12. Click the **Turn it on** checkbox (optional but you will need to turn the connector on later).
13. Click **Next**.

Connector name

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

Name * ①

Description ②

What do you want to do after connector is saved? ⓘ

☒ Turn it on ③

④

14. On the **Use of connector** section select **Only when I have a transport rule set up that redirects messages to this connector**.
15. Click **Next**.

Use of connector

Specify when you want to use this connector.

1

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

☐ Only when email messages are sent to these domains

Back Next 2

16. On the **Routing** section select the **Route email through these smart hosts** radio button.
17. In the textbox, type the appropriate domain for your DataMotion platform server (appropriate connector domains [above](#)).
18. Click the plus icon to add the smart host.

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.

☐ Use the MX record associated with the partner's domain

☒ Route email through these smart hosts 1

scpusv7.datamotion.com 2

+ 3

NOTE: If you are not sure which smart host domain you should use (list [above](#)) contact DataMotion support at support@datamotion.com as entering an incorrect domain will cause the entire connector to fail.

19. The smart host will be created.

20. Click **Next**.

☐ Use the MX record associated with the partner's domain

☒ Route email through these smart hosts

Example: myhost.contoso.com or 192.168.3.2

scpusv7.datamotion.com

Back Next

21. On the **Security restrictions** section select the following:

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

23. Issued by a trusted certificate authority (CA).

24. Click Next.

Security restrictions

How should Office 365 connect to your partner organization's email server?

1 ☒ 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

2 ☒ Issued by a trusted certificate authority (CA)

☐ Add the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or *.contoso.com

Back Next 3

25. On the **Validation email** section:

- » Enter an appropriate email address.
- » Click the plus icon.

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.

1 + 2

26. Click the **Validate** button.

27. When validation completes click **Next**.

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.

+

🗑️

Validate 1

Back Next 2

28. On the **Review connector** screen all the details you entered for the connector will be displayed.
29. Review and ensure these are correct.
30. Click the **Create connector** button.

Review connector

Mail flow scenario

From: Office 365
To: Partner organization

Name

dm

Status

Turn it off after saving
[Edit name](#)

Use of connector

Use only when I have a transport rule set up that redirects messages to this connector.
[Edit use](#)

Routing

Route email messages through these smart hosts: `scpusv7.datamotion.com`
[Edit routing](#)

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).
[Edit restrictions](#)

Back

Create connector

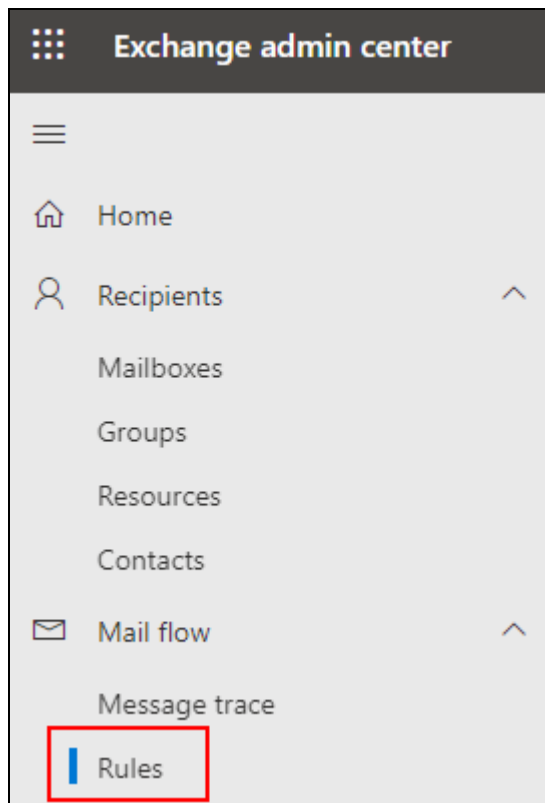
31. Once the connector is created ensure its Status is set to On and these steps will be completed.

If you have not done so already, you will need to create a rule in your mail flow to utilize the connector created in this section. To create a mail flow rule, see the Use Microsoft Exchange to Create a Rule with a Secure Tag section.

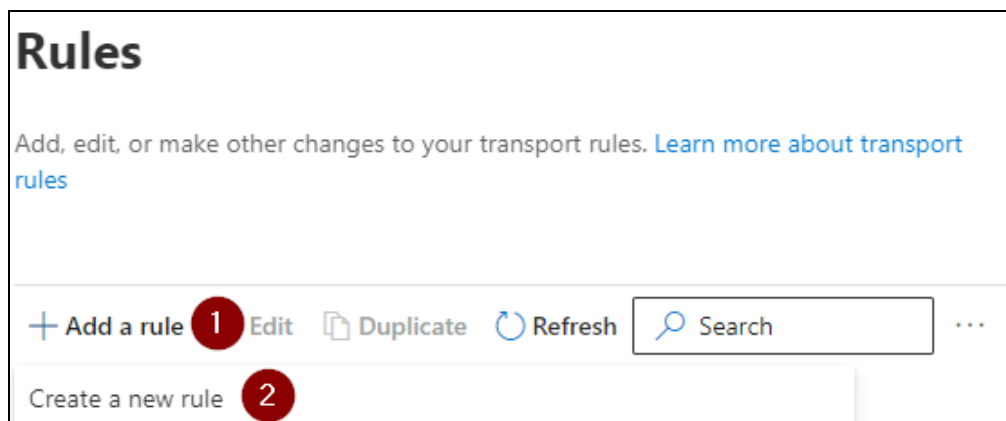
USE MICROSOFT EXCHANGE TO CREATE A RULE WITH A SECURE TAG

The following instructions describe setting up a Microsoft 365 mail flow rule to utilize the connector created in the [Create a Connector to Route Messages to DataMotion](#) section.

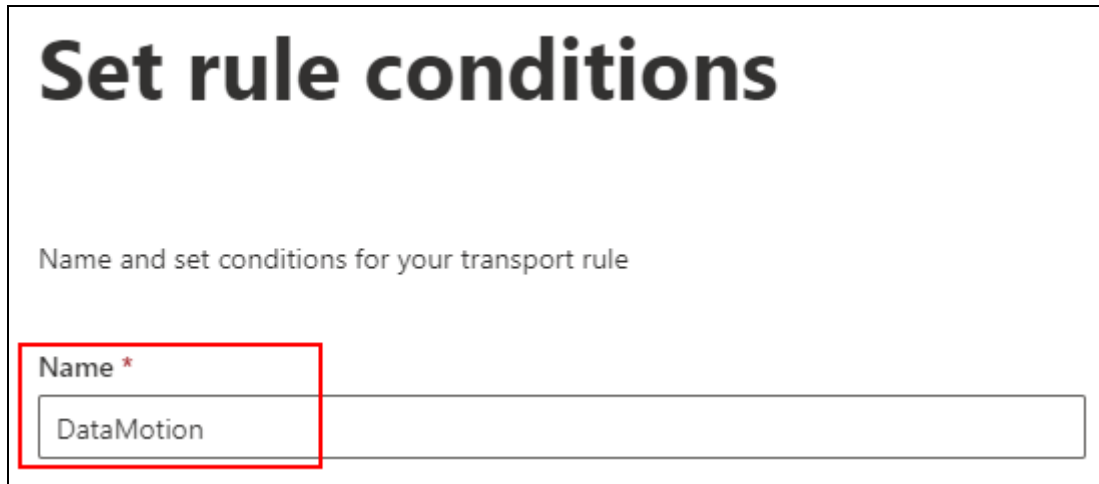
1. From your **Exchange admin center**:
2. Select **Rules** from the menu on the left.



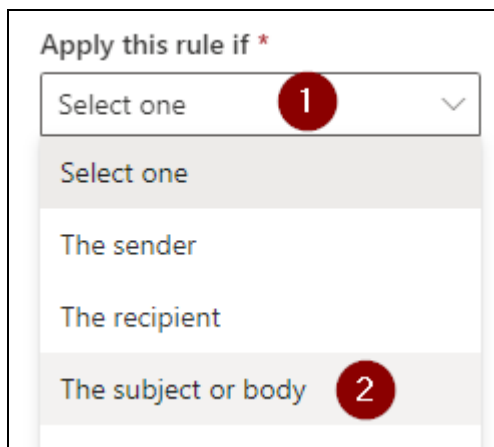
3. Select the **Add a rule** button click **Create a new rule**.



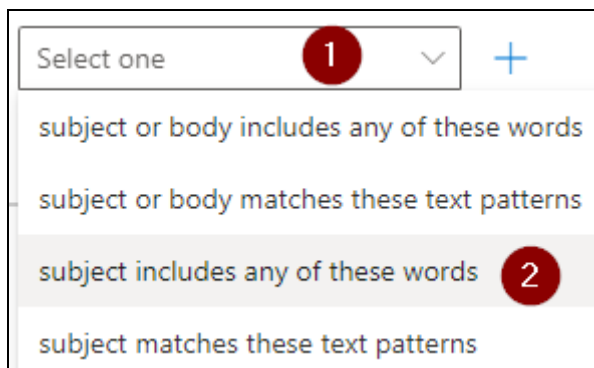
4. The New transport rule screens will open.
5. On the **Set rule conditions** screen add a **Name**.



6. Click the drop-down field under **Apply this rule if**.
7. Select **The subject or body**.



8. In the drop-down to the right select **subject includes any of these words**.



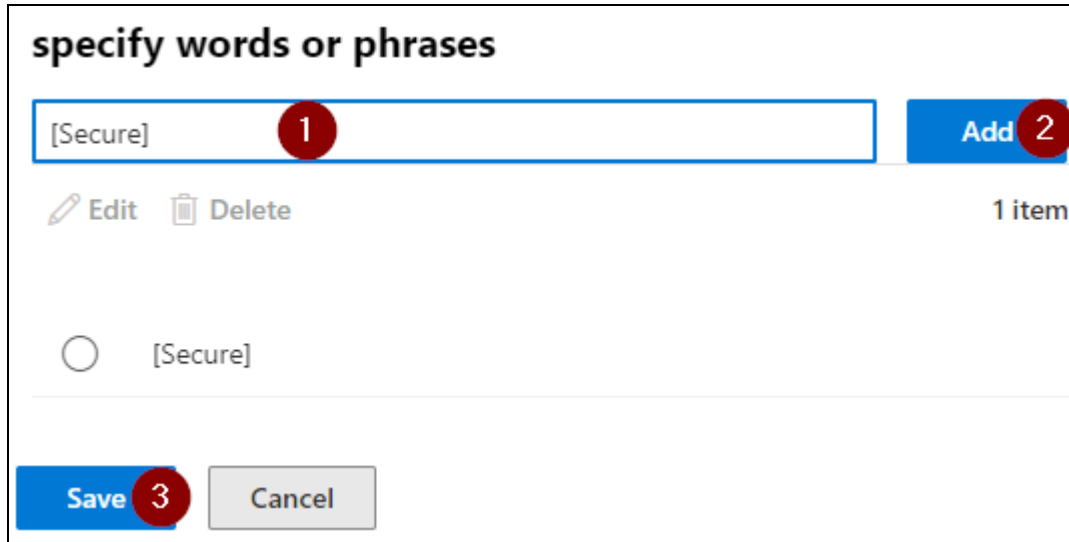
9. In the specify words or phrases screen is displayed. In the text box, type **[Secure]**.

NOTE: This specifies the tag used in the email subject line for identifying sensitive email that will be routed to the DataMotion platform's server.

10. Click the **Add** button.

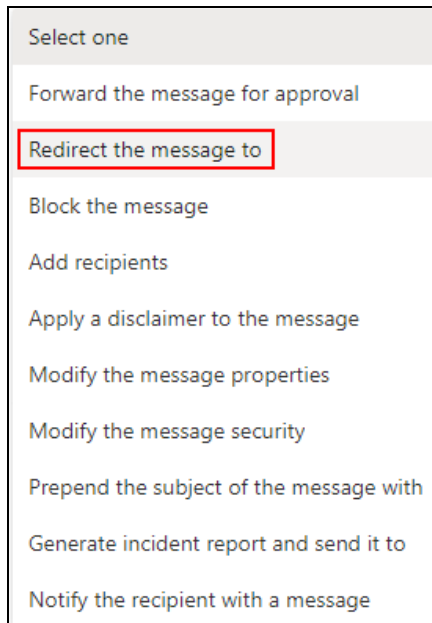
» [Secure] will appear as a selectable item.

11. Click the **Save** button.

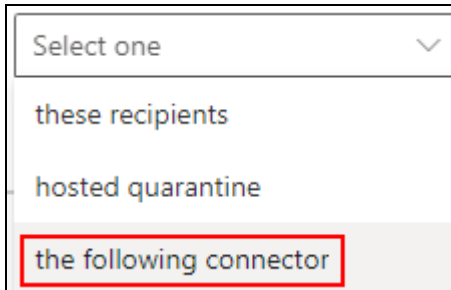


12. Click the **Do the following** drop down.

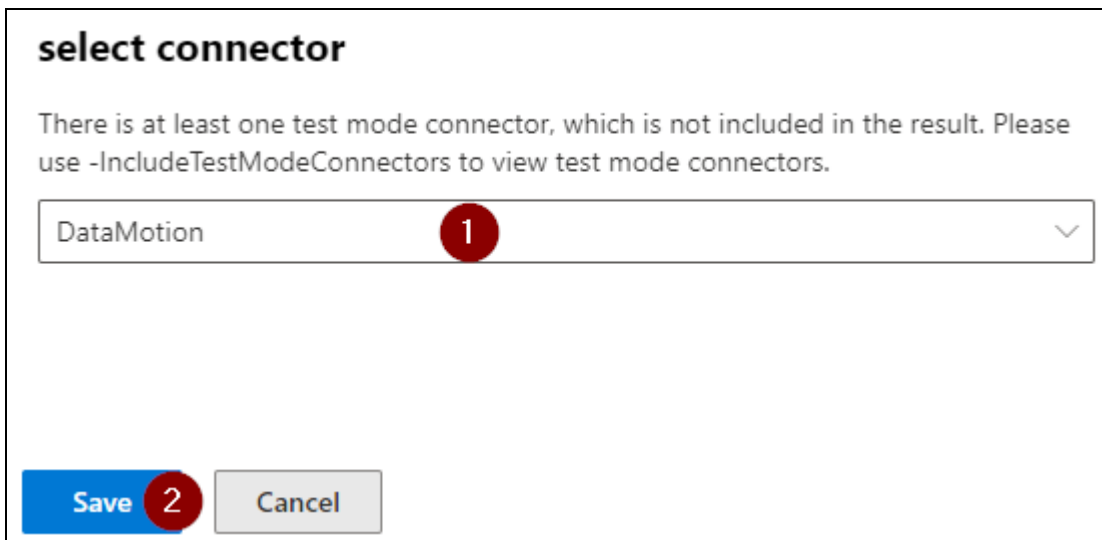
13. Select **Redirect the message to**.



14. Select the drop-down to the right.
15. Select **the following connector**.



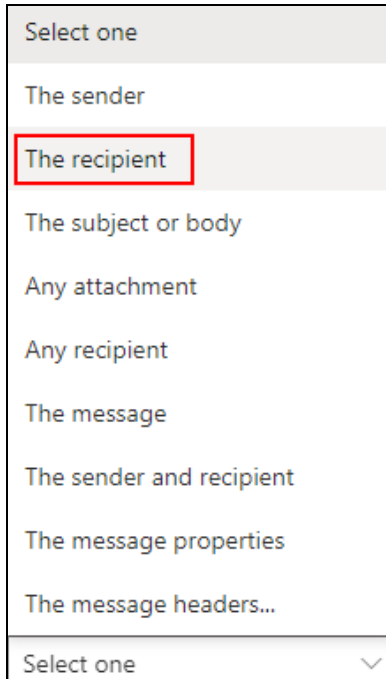
16. In the **select connector** screen choose your connector.
17. Click the **Save** button.



18. (Optional) add an exception to the rule for communication inside of the organization by performing the following:

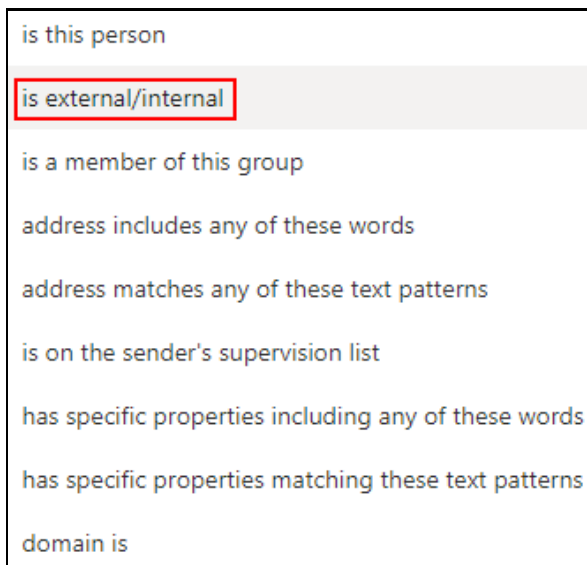
a. Click the drop-down field under **Except if**.

b. Select **The recipient**.



A screenshot of a drop-down menu. The menu is open, showing a list of options. The option 'The recipient' is highlighted with a red rectangular box. The options listed are: 'Select one', 'The sender', 'The recipient', 'The subject or body', 'Any attachment', 'Any recipient', 'The message', 'The sender and recipient', 'The message properties', 'The message headers...', and 'Select one' at the bottom with a downward arrow.

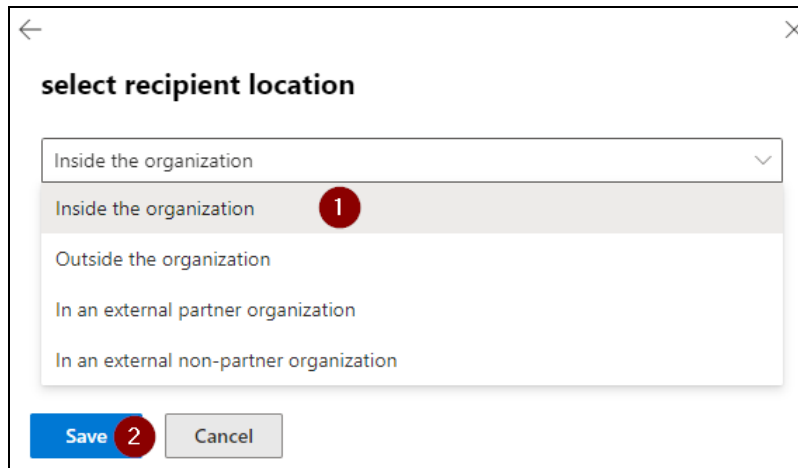
c. In the drop-down to the right select **is external/internal**.



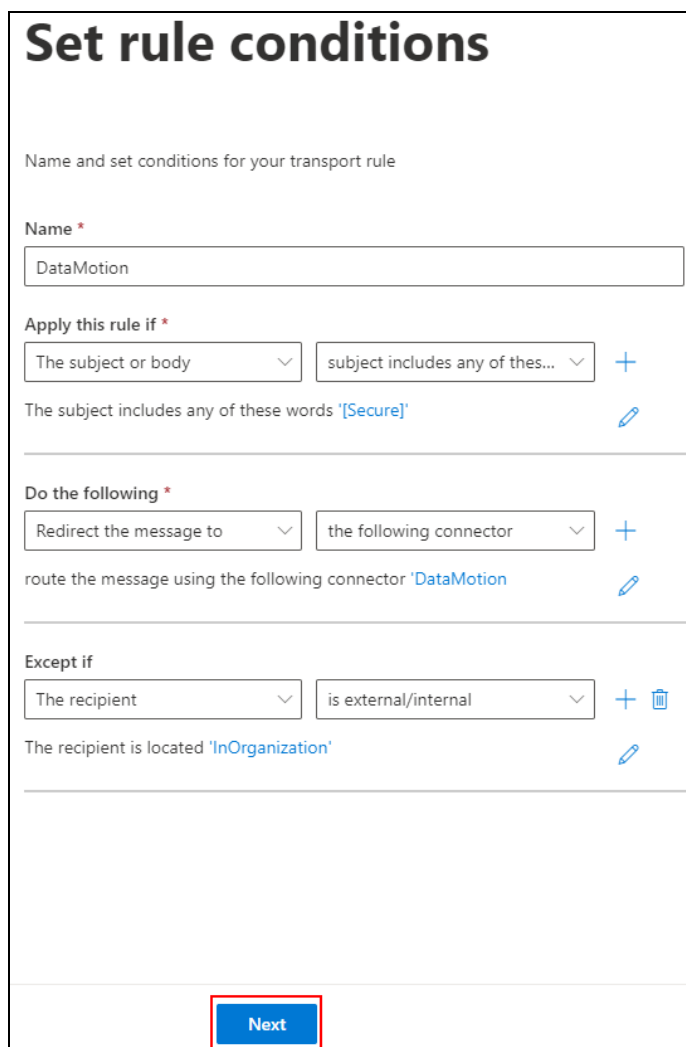
A screenshot of a drop-down menu. The menu is open, showing a list of options. The option 'is external/internal' is highlighted with a red rectangular box. The options listed are: 'is this person', 'is external/internal', 'is a member of this group', 'address includes any of these words', 'address matches any of these text patterns', 'is on the sender's supervision list', 'has specific properties including any of these words', 'has specific properties matching these text patterns', and 'domain is'.

d. On the **select recipient location** screen, click the drop-down and choose Inside the organization.

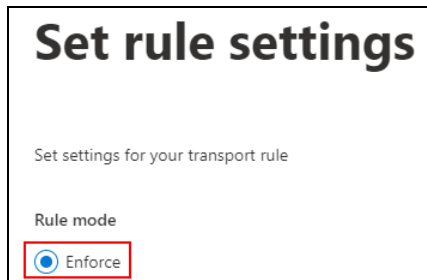
- e. Click the **Save** button.



19. Review the connector to ensure everything has been entered and click **Next**.



20. On the **Set rule settings** page, you can set additional options, but it is recommended to set Rule mode to Enforce.



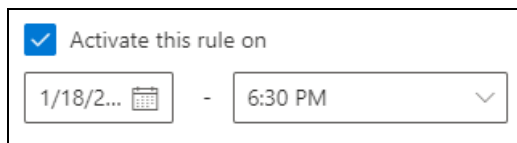
Set rule settings

Set settings for your transport rule

Rule mode

☒ Enforce

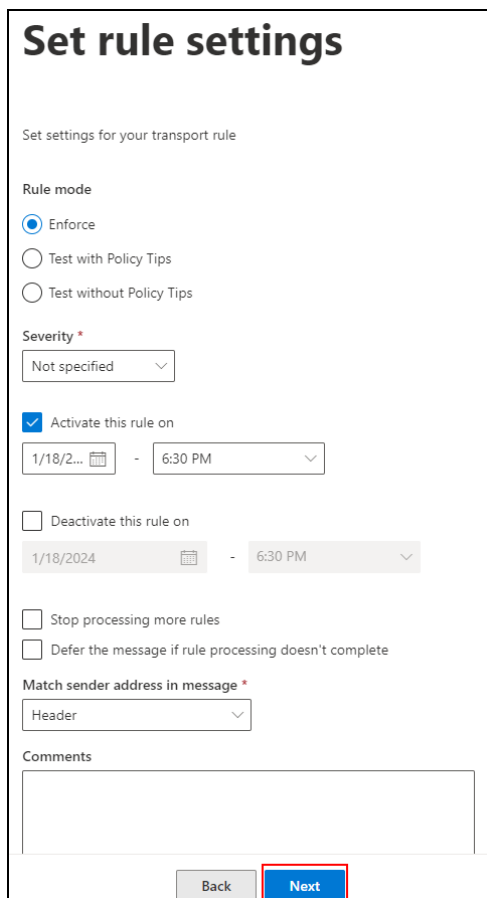
21. (Optional) you can choose an activation date to avoid having to activate the rule manually if desired.



☒ Activate this rule on

1/18/2... - 6:30 PM

22. Review and click **Next**.



Set rule settings

Set settings for your transport rule

Rule mode

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

Severity *

Not specified

☒ Activate this rule on

1/18/2... - 6:30 PM

☐ Deactivate this rule on

1/18/2024 - 6:30 PM

☐ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message *

Header

Comments

Back Next

23. Review the finalized rule and click **Finish**.

Review and finish

After your finish creating this rule, it is turned off by default until you turn it on from the Rules page

Rule name
DataMotion

Rule comments

Rule conditions	Rule settings
Apply this rule if The subject includes any of these words '[Secure]'	Mode Enforce
Do the following route the message using the following connector 'DataMotion SecureMail'	Set date range 1/18/2024 06:30 PM -
Except if The recipient is located 'InOrganization'	Priority 21
Edit rule conditions	Severity Not specified
	For rule processing errors Ignore
	Stop processing more rules false
	Edit rule settings

BackFinish

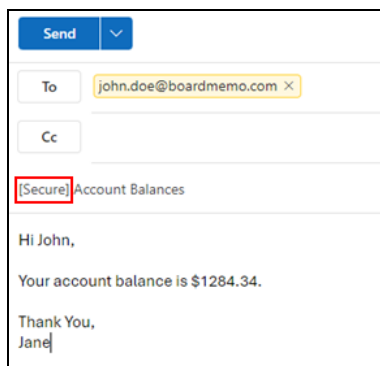
This completes the setup for adding a Mail flow rule. Please ensure you activate your rule if you did not set an activation date during the creation process.

SEND A SECURE MESSAGE (TO CONFIRM OPERATION)

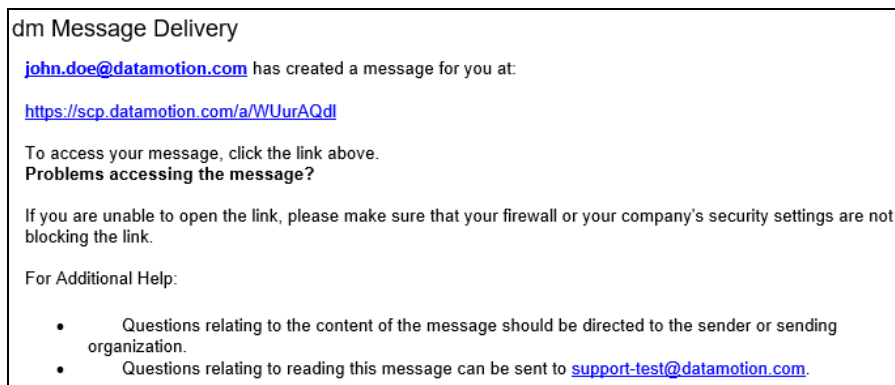
The following information illustrates how the Exchange rule works when sending a secure message.

NOTE: For the secure messaging to work, you MUST have a LICENSED DataMotion SMC account. If you do not have one, please contact DataMotion Sales to set one up.

1. From your Microsoft 365 account, create a new message like the one shown here. Make sure to type **[Secure]** as the first word in the Subject line. (This is the tag to identify the email as a DataMotion SMC message.)



2. Click **Send** to send the message. The recipient should then receive an email containing a DataMotion SMC notification similar to the following.



3. The recipient can click on the link and login to the account to retrieve the secure message. If this is the first time receiving a DataMotion SMC message, the recipient will create a new password for their account.

CREATING A CONNECTOR AND AN ASSOCIATING RULE FOR INBOUND SECURE MESSAGES (OPTIONAL)

In certain configurations typically when plain text delivery is enabled, it is advised to configure a separate connector and an associating rule to discern internal communications using the DataMotion Secure Message Center from regular messages within your organization.

CONNECTOR IP ADDRESS REQUIREMENTS

Similar to the previous connector's steps, when you are creating this connector you will be required to enter an IP address. The IP address that should be entered will vary depending on geographical region and are listed below:

- CA region: **20.104.180.171**
- US region: **20.127.125.212**

CREATING A CONNECTOR FOR INTERNAL SECURE COMMUNICATIONS

This section describes creating the connector for internal secure communications using DataMotion SMC.

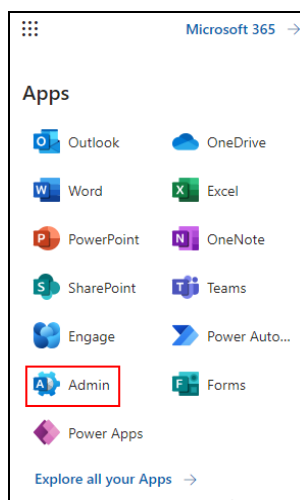
NOTE: These steps assume you have already logged into Microsoft 365 as an administrator with Exchange Admin privileges or greater.

During setup it is required that an IP address be entered for completing the connector creation process.

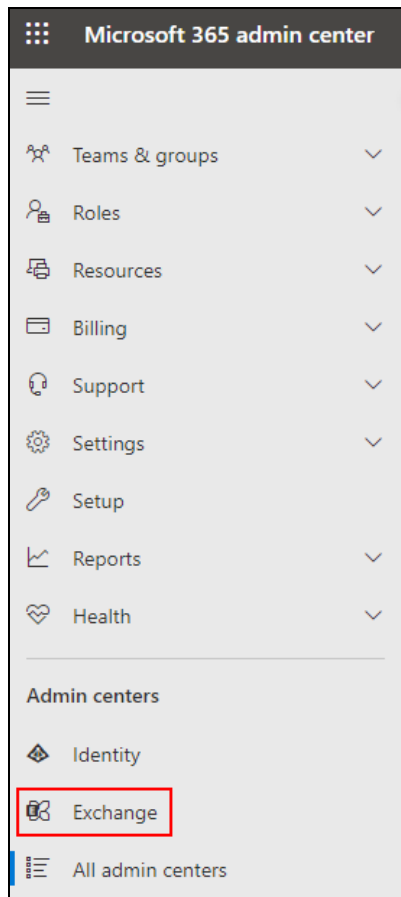
1. Open the Apps menu by clicking the 3x3 dots icon (typically looks like the image below).



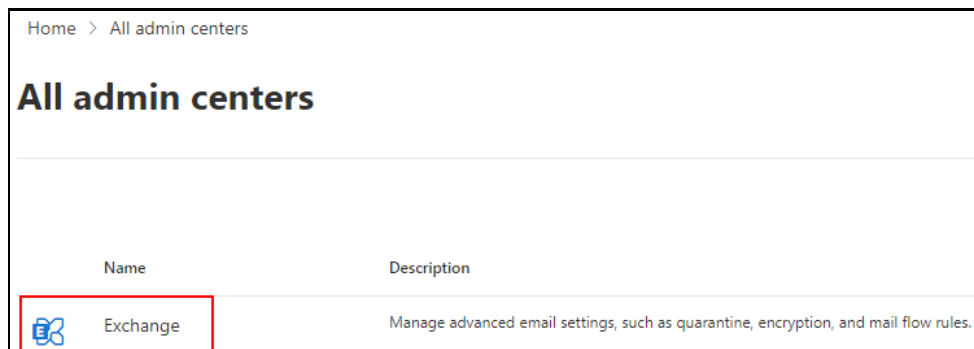
2. Select **Admin** (your available Apps and their order may differ).



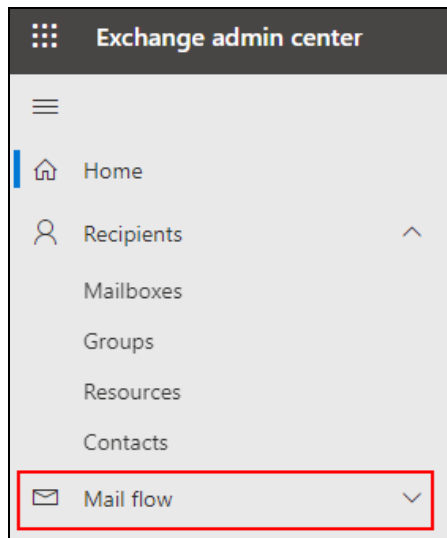
- Under the **Microsoft 365 admin center** pull out scroll down to the **Admin centers** section, and select **Exchange**.



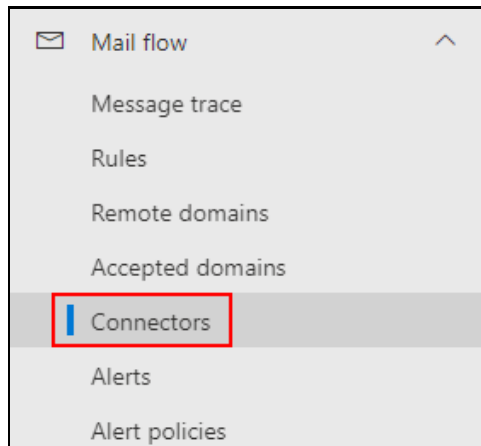
- If Exchange does not appear initially, you can select **All admin centers** and then Exchange.



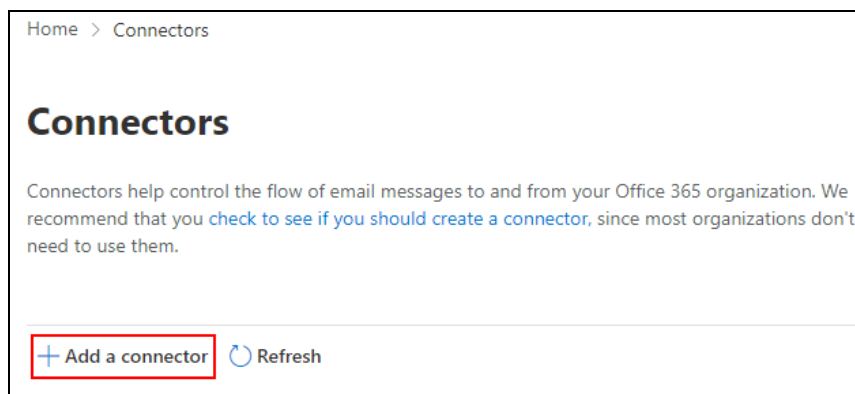
5. Once **Exchange admin center** opens, click the **Mail flow** section on the left side of the screen.



6. Click **Connectors**.



7. On the **Connectors** screen, click the **Add a connector** button to create a new connector.



8. On the New connector screen select **Your organization's email server**.

The screenshot shows the 'Add a connector' wizard. On the left, a progress bar has four steps: 'New connector' (selected), 'Name', 'Authenticating sent email', and 'Review connector'. The main area is titled 'New connector' and contains the instruction: 'Specify your mail flow scenario, and we'll let you know if you need to set up a connector.' Under 'Connection from', there are three radio buttons: 'Office 365', 'Your organization's email server' (which is selected and highlighted with a red box), and 'Partner organization'. Under 'Connection to', there is one radio button: 'Office 365'.

» Connection to can only be set to Office 365.

9. Click Next.
10. Give the connector a Name.
11. Give it a Description.
12. Click Turn it on (optional but you will need to enable the connector later).
13. Click Next.

The screenshot shows the 'Add a connector' wizard at the 'Connector name' step. The progress bar on the left now has 'Name' selected. The main area is titled 'Connector name' and contains the instruction: 'This connector lets Office 365 deliver messages from your organization's email server.' There is a text input field for 'Name *' with the value 'From Secure Message Center' (marked with a red circle 1). Below it is a text area for 'Description' with the value 'Receive Plain Text messages and notifications from Secure Message Center.' (marked with a red circle 2). At the bottom, there is a section 'What do you want to do after connector is saved?' with two checkboxes: 'Turn it on' (checked, marked with a red circle 3) and 'Retain internal Exchange email headers'. At the very bottom, there are 'Back' and 'Next' buttons, with the 'Next' button highlighted and marked with a red circle 4.

14. On the Authenticating sent email screen select the **By verifying that the IP address...** radio button.
15. Enter the appropriate IP address for your region.
 - » The appropriate IP addresses are highlighted *above*.
16. Click the plus icon.
 - » The IP address shall be added.
17. Click Next.

The screenshot shows the 'Add a connector' wizard with four steps in the left sidebar: 'New connector' (checked), 'Name' (checked), 'Authenticating sent email' (active), and 'Review connector' (unchecked). The main content area is titled 'Authenticating sent email' and asks 'How should Office 365 identify email from your email server?'. It provides two options: '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)' (unselected) and 'By verifying that the IP address of the sending server matches one of the following IP addresses, which belong exclusively to your organization' (selected). The selected option has a text input field with an example '10.5.3.2 or 10.3.1.5/24' and a plus icon (labeled 1 and 2). Below the input field, the IP address '20.104.180.171' is listed with a trash icon. At the bottom, there are 'Back' and 'Next' buttons, with the 'Next' button labeled 3.

18. On the Review connector screen ensure all information has been entered correctly.

19. Click **Create connector**.

The screenshot shows the 'Add a connector' screen in the Exchange administrator interface. On the left, a vertical progress bar indicates the steps: 'New connector' (checked), 'Name' (checked), 'Authenticating sent email' (checked), and 'Review connector' (active). The main area is titled 'Review connector' and contains the following information:

- Mail flow scenario**
 - From: Your organization's email server
 - To: Office 365
- Name**
 - From Secure Message Center
- Status**
 - Turn it on after saving
 - Don't retain internal Exchange email headers
 - [Edit name](#)
- How to identify email sent from your email server**
 - Identify incoming messages from your email server by verifying that the sending server's IP address is within these IP address ranges: 20.127.125.212, and the sender's or recipient's email address is an accepted domain for your organization.
 - [Edit sent email identity](#)

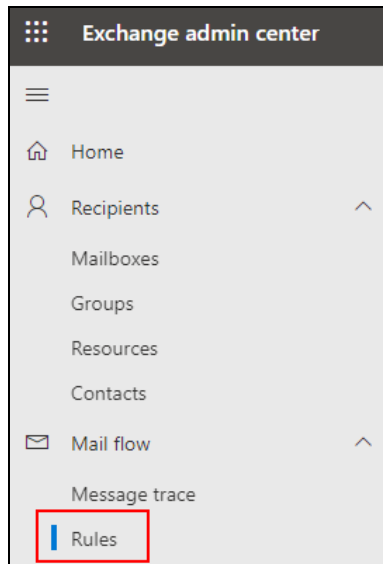
At the bottom, there are two buttons: 'Back' and 'Create connector'. The 'Create connector' button is highlighted with a red rectangle.

Now that the connector has been created a mail flow rule will be needed to utilize it. Please do not leave the Exchange administrator interface as the setup will continue from within there.

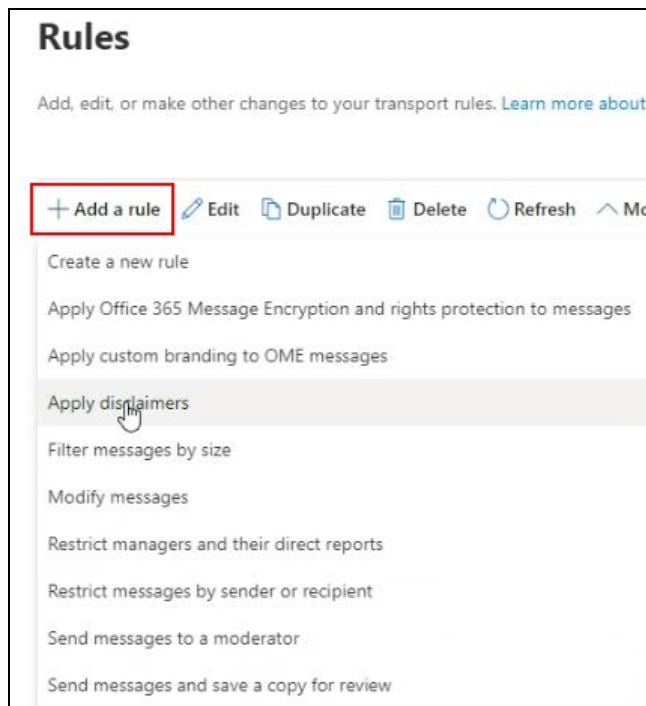
CREATING THE MAIL RULE FOR INTERNAL SECURE COMMUNICATIONS

This section shall cover creating the mail rule associated with the connector created in the previous section.

1. From your **Exchange admin center**:
3. Select **Rules** from the menu on the left.



4. Click Add a rule
5. Select Apply disclaimers.



6. On the Set rule conditions screen give the rule a Name.

Set rule conditions

Name and set conditions for your transport rule

Name *

DataMotion

7. For the **Apply this rule if** drop-down select **IP address is any of these ranges or exactly matches**.

IP address is in any of these ranges or... ▾

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

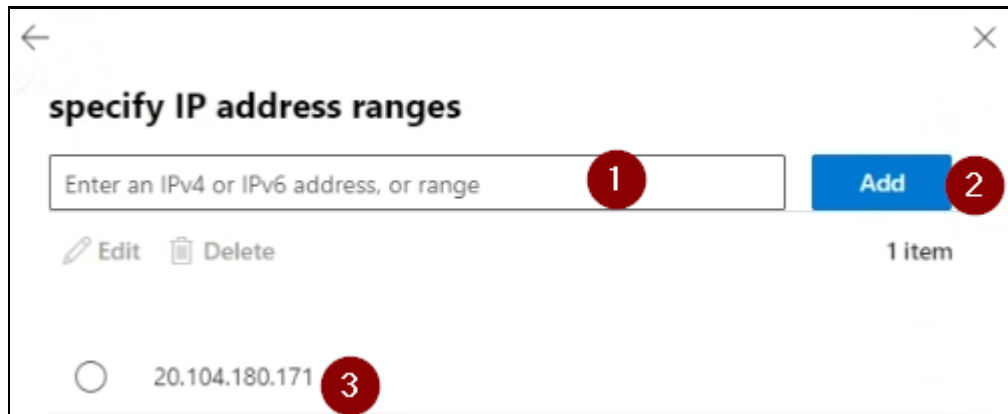
has specific properties matching these text patterns

IP address is in any of these ranges or exactly matches

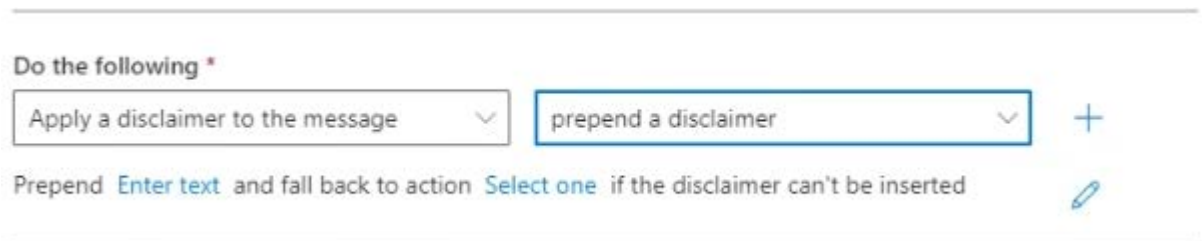
domain is

8. In the drop-down to the right select **The sender**.

9. In the specify IP address ranges screen enter the following:
 - » Enter the appropriate IP address for your region (it should match the one entered during connector setup).
 - » Click Add.
 - » The IP address will be added.
 - » Click Save.



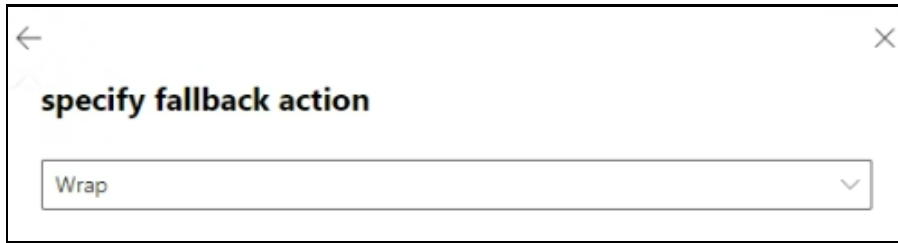
10. For the Do the following section select the following:
 - » For the left drop-down select Apply a disclaimer to the message.
 - » For the right drop-down select prepend a disclaimer.



11. To enter the disclaimer message select **Enter text**.
12. In the specify disclaimer text screen enter a disclaimer in the text box (please note that html is supported).



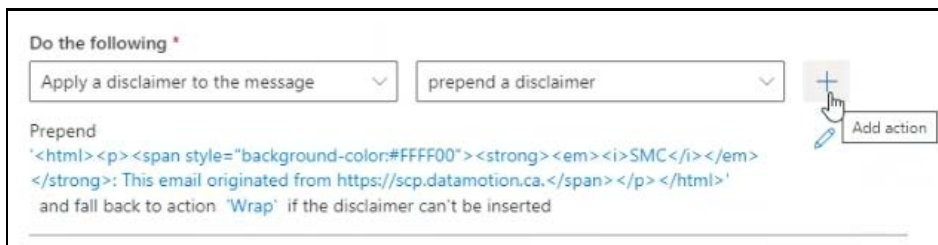
13. Create a fallback action by choosing Select one.
14. In the **specify fallback action** screen choose Wrap in the drop-down.



← specify fallback action ×

Wrap ▾

15. We are going to create a second **Do the following** set of options so click the **Add action** plus icon.



Do the following *

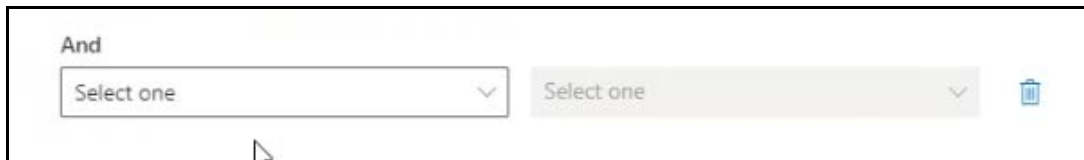
Apply a disclaimer to the message ▾ prepend a disclaimer ▾ + Add action

Prepend

'<html><p><i>SMC</i></p></html>': This email originated from https://scp.datamotion.ca.</p></html>'

and fall back to action 'Wrap' if the disclaimer can't be inserted

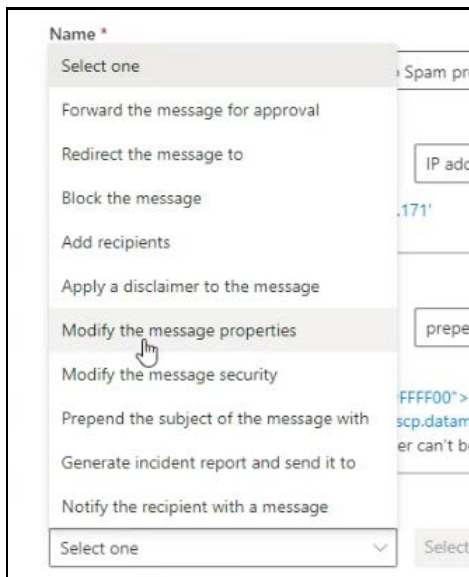
16. You should get an empty **And** section:



And

Select one ▾ Select one ▾ 🗑️

17. For the Select one drop-down on the left of the And section select Modify the message properties.



Name *

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
- Generate incident report and send it to
- Notify the recipient with a message

Select one ▾

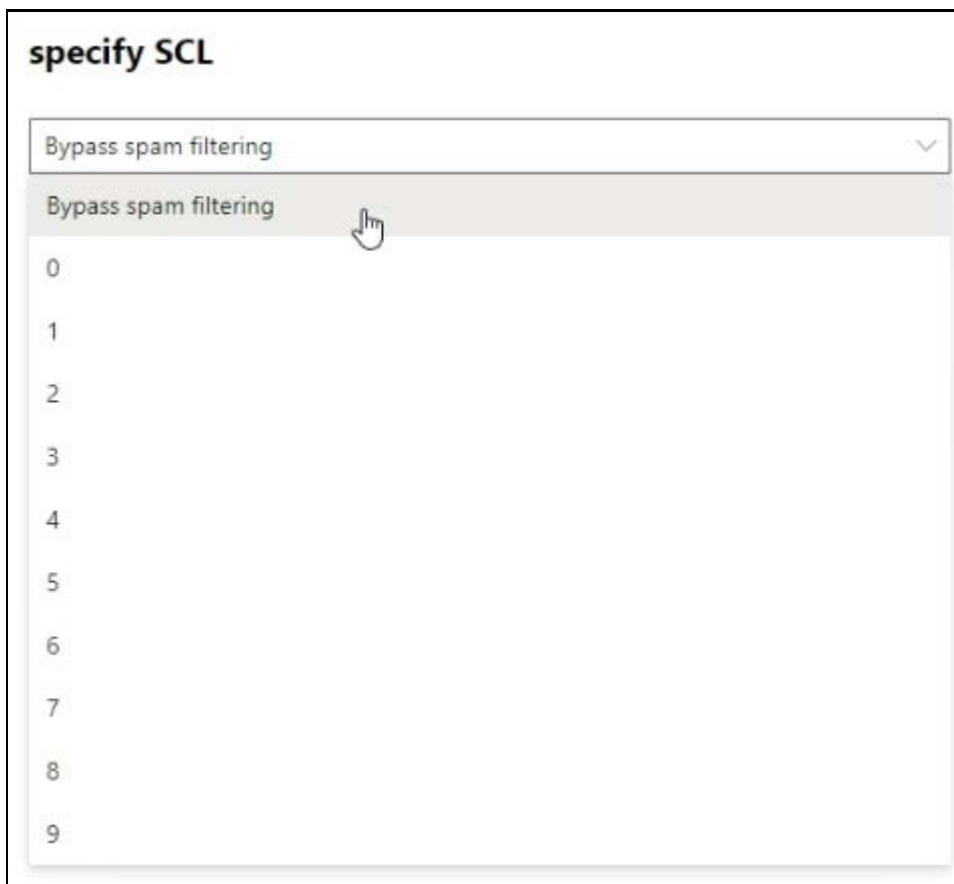
18. For the drop-down to the left select set the spam confidence level (SCL).



Select one

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

19. In the specify SCL screen select Bypass spam filtering from the drop-down.



specify SCL

Bypass spam filtering

Bypass spam filtering

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9

20. Delete the Except if section (optional).

21. Click Next.

22. On the set rule settings page perform the following:
- » Set **Rule mode** to **Enforce**.
 - » Select Stop processing more rules (optional, depends on your organization's rule behavior).
 - » Click Next.

New transport rule

- ✓ Set rule conditions
- Set rule settings
- Review and finish

Set rule settings

Set settings for your transport rule

Rule mode

☒ Enforce **1**

☐ Test with Policy Tips

☐ Test without Policy Tips

Severity *

Not specified

☐ Activate this rule on

2/2/2024 - 2:00 PM

☐ Deactivate this rule on

2/2/2024 - 2:00 PM

☒ Stop processing more rules **2**

☐ Defer the message if rule processing doesn't complete

Match sender address in message *

Header

Comments

Back Next **3**

23. Review the rule settings and click Finish to create the rule.

New transport rule

- Set rule conditions
- Set rule settings
- Review and finish**

Review and finish

After your finish creating this rule, it is turned off by default until you turn it on from the Rules page

Rule name
Secure Message Center Add Banner and Skip Spam processing.

Rule comments

Rule conditions

Apply this rule if
Sender's IP address is in the range '20.104.180.171'

Do the following
Prepend '<html><p><i>SMC</i>: This email originated from https://scp.datamotion.ca.</p></html>'
and fall back to action 'Wrap'
if the disclaimer can't be inserted
Set the spam confidence level (SCL) to '-1'

Except if
[Edit rule conditions](#)

Rule settings

Mode
Enforce

Set date range
Specific date range is not set

Priority
22

Severity
Not specified

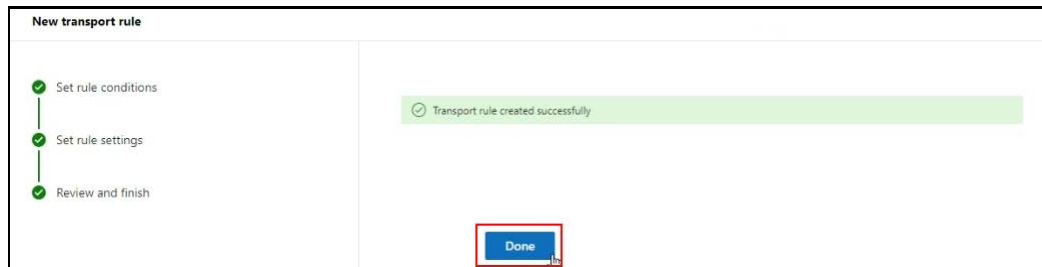
For rule processing errors
Ignore

Stop processing more rules
true

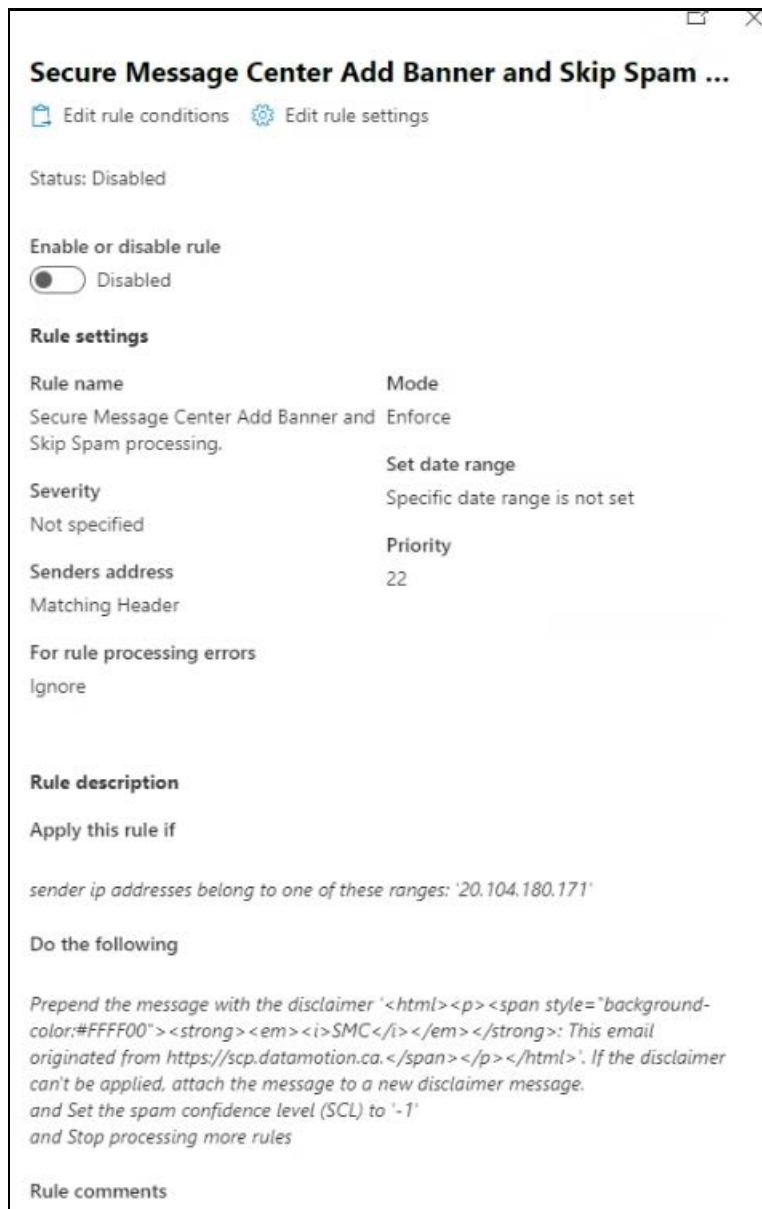
[Edit rule settings](#)

[Back](#) [Finish](#)

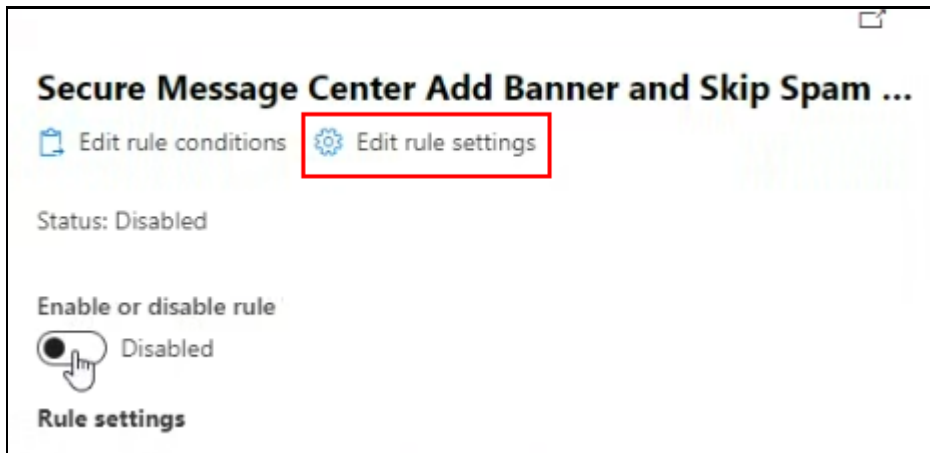
24. Once the rule is created click Done.



25. Once finished, locate the rule that was just created and edit the rule. This should look similar to the following:



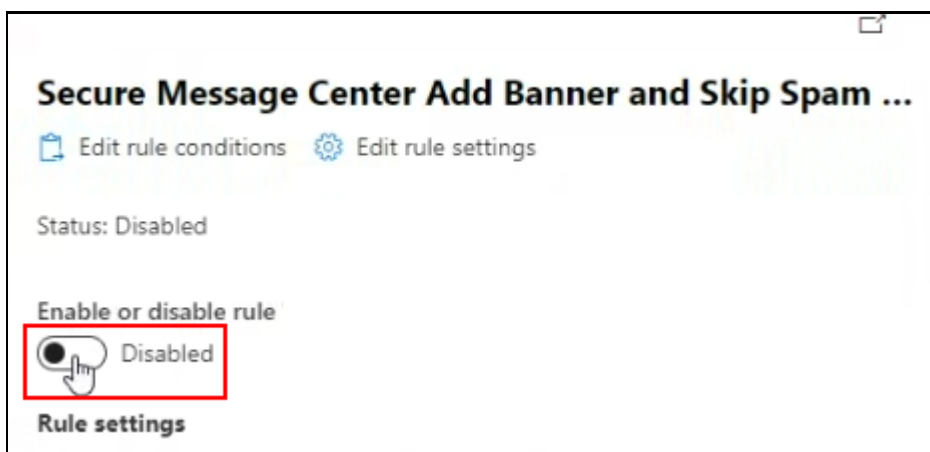
26. Click on Edit rule settings.



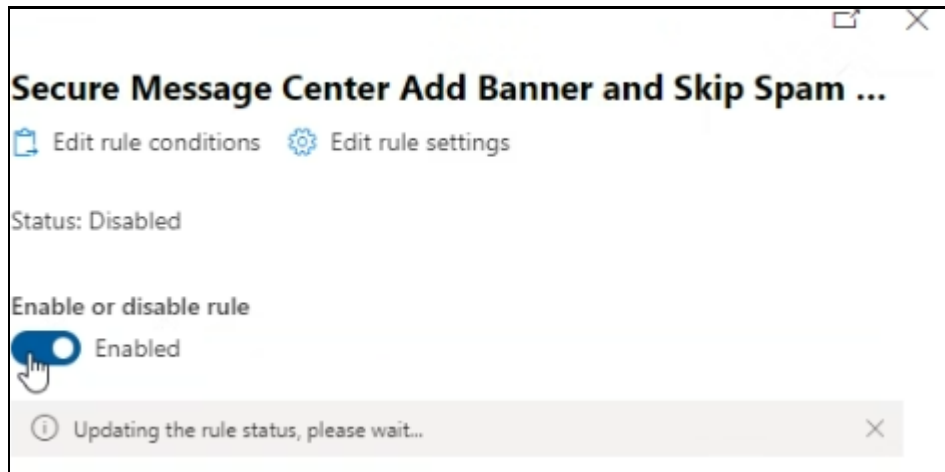
27. Change the Priority to 0 and save.



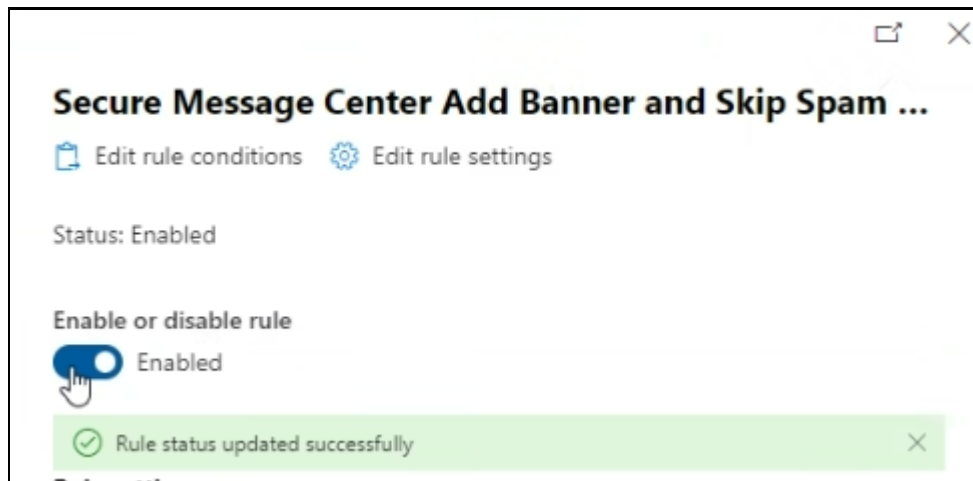
28. Click the Enable or disable rule toggle.



29. There will be a short propagation period like the below:

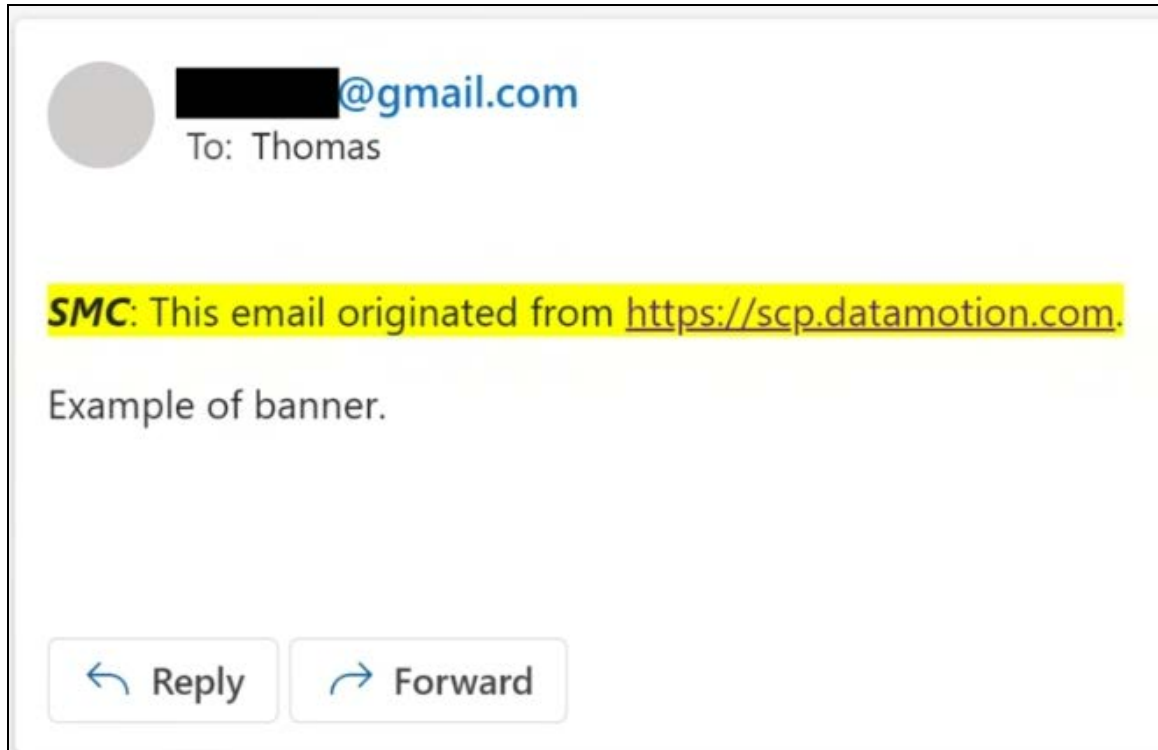


30. Once finished the rule will be enabled and it will look like the below:



SEND A SECURE MESSAGE INTERNALLY TO ENSURE PERSONNEL RECEIVE THE APPROPRIATE BANNER

While optional, you should send a secure message internally from one employee to another to ensure that the connector and rule made in the previous sections function as expected. Simply create a secure message using Outlook from within Microsoft 365 and send it to another employee. The result should show something like the following:



* * *

This represents the end of the *DataMotion Secure Message Center Integration Guide for Microsoft 365*.