



DataMotion SecureMail Setup Guide for Microsoft Office 365

June 3, 2020
Part # 050013-05

Copyright © 2008 - 2020, 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 SecureMail Setup Guide for Microsoft Office 365 v5

Publication Date: June 3, 2020

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 DATAMOTION SECUREMAIL..... 7

INTENDED AUDIENCE 7

HOW TO USE THIS PUBLICATION 8

RELATED INFORMATION 8

DataMotion Documentation 8

1 INTRODUCTION **9**

DATAMOTION SECUREMAIL FOR OFFICE 365 9

Important Note About the Secure Tag..... 10

2 OVERVIEW OF THE SETUP **11**

SETUP PROCEDURE (SUMMARY) 11

3 SET UP MICROSOFT OFFICE 365 FOR DATAMOTION SECUREMAIL 12

REVIEW THE REQUIREMENTS	12
SIGN IN TO OFFICE 365.....	12
CREATE A CONNECTOR TO ROUTE EMAIL TO DATAMOTION SECUREMAIL	15
USE MICROSOFT EXCHANGE TO CREATE A RULE WITH A SECUREMAIL TAG	24
SEND A SECURE EMAIL (TO CONFIRM OPERATION)	28
OPTIONAL: USE THE DATAMOTION SECUREMAIL PLUG-IN FOR MICROSOFT OUTLOOK.....	29
FINAL STEP: AUTHORIZE DATAMOTION AS AN EMAIL SENDER.....	29

4 ADDITIONAL TECHNICAL INFORMATION 30

DATAMOTION IP WHITELIST FOR MICROSOFT OFFICE 365	30
--	----

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 5

Chapter 3: *Set Up Microsoft Office 365 for DataMotion SecureMail*

- ***Final Step: Authorize DataMotion as an Email Sender*** (below)
 - » Changed the SPF record in this section to match the new IP address.

Version 4

Chapter 3: *Set Up Microsoft Office 365 for DataMotion SecureMail*

- ***Review the Requirements*** (on page 12)
 - » Removed references to the Office 365 versions that include DLP settings as these no longer apply to what's supported in the 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 Email to DataMotion SecureMail*** (on page 15)
 - » 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: *Set Up Microsoft Office 365 for DataMotion SecureMail*

-
- ***Use Microsoft Exchange to Create a Rule with a SecureMail Tag*** (on page 23)

- 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 DATAMOTION SECUREMAIL

This publication describes how to set up DataMotion SecureMail for use with Microsoft Office 365. DataMotion SecureMail provides easy-to-use encrypted email messaging and data transfer via the Internet for protecting all of the important information flowing between you, your business partners and your clients.

SecureMail protects sensitive messages 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. It works with popular email clients such as Microsoft Outlook, as well as on the iPhone and other mobile devices, and it is intuitive for senders and recipients, so it can be up and running in minutes with no outside IT support. With integrated large file support, DataMotion SecureMail seamlessly delivers documents, images, and other files up to 2 GB in size, eliminating a significant bottleneck in data exchange.

Providing effortless secure sending 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 SecureMail 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 SecureMail for Microsoft Office 365.

Chapter 2) Overview of the Setup

Provides a synopsis of the setup procedures.

Chapter 3) Set Up Microsoft Office 365 for DataMotion SecureMail

Provides step-by-step instructions on how to set up Microsoft Office 365 for use with DataMotion SecureMail.

Chapter 4) Additional Technical Information

Provides additional technical information for using DataMotion SecureMail with Microsoft Office 365.

RELATED INFORMATION

DATAMOTION DOCUMENTATION

- *DataMotion SecureMail Software Development Kit Reference Manual* (part # 050030)
Documents the Application Programming Interfaces (APIs), and system development, maintenance, and administration tools for developers.
- *DataMotion SecureMail User Guide* (part # 050004)
Provides instructions for using the products.
- *DataMotion SecureMail 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 Customer Service for more information.

1

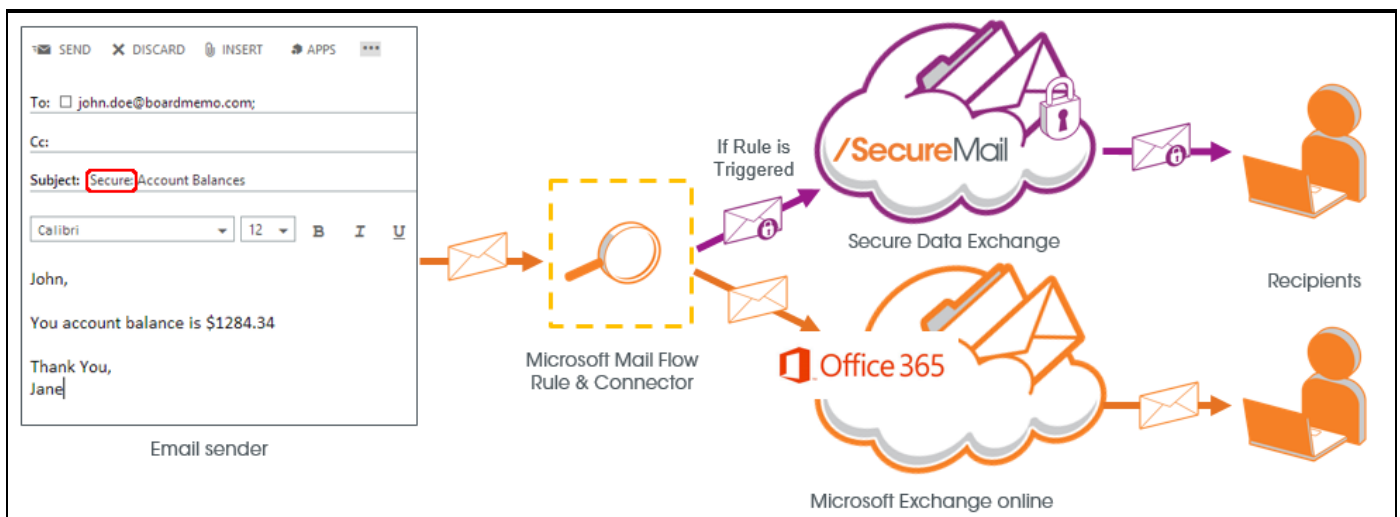
Introduction

DATAMOTION SECUREMAIL FOR OFFICE 365

DataMotion SecureMail 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 SecureMail for Microsoft Office 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 SecureMail for Office 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 SecureMail with Office 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 SecureMail Tag section) will route the message to a connector (created in the Create a Connector to Route Email to DataMotion SecureMail 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 SecureMail host, which then delivers it securely to recipients. Messages that are not sensitive are sent through the cloud-based Office 365 Exchange Online server, which does not guarantee secure delivery.

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

IMPORTANT NOTE ABOUT THE SECURE TAG

Throughout this document the Secure: tag that is used is simply an example of how the tag is created and used in the Office 365 setup. There is no restriction to what the tag must look like when setting up this process for use in real time. When going through the instructions that refer to the Secure: tag in this guide, you can simply substitute it with the tag you want. If desired it is also possible to have as many tags as you deem necessary for a variety of different purposes.

2

Overview of the Setup

DataMotion SecureMail for Office 365 is easily integrated into the Office 365 environment. It uses Exchange Mail Flow Rules and Connectors to route email based on the presence of a “Secure: ” tag. Once configured, the DataMotion SecureMail for Office 365 works out of the box, with no extra applications required to be installed 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. ***Sign in to Office 365*** (on page 12):
Make sure to sign into Office 365 as an administrator.
3. ***Create a Connector to Route Email to DataMotion SecureMail*** (on page 15):
Create an outbound connector to set up email routing to the DataMotion SecureMail gateway. This enables secure messages to be processed properly by the DataMotion SaaS.
4. ***Use Microsoft Exchange to Create a Rule with a SecureMail Tag*** (on page 23)
Create a Microsoft Exchange rule to scan for a subject line tag of “Secure: ”.
5. ***Send a Secure Email (to Confirm Operation)*** (on page 28):
Confirm the operation by creating and sending a secure message.
6. ***Optional: Use the DataMotion SecureMail Plug-in for Microsoft Outlook*** (on page 29):
Review the information for using the Microsoft Outlook plug-in.
7. ***Final Step: Authorize DataMotion as an Email Sender*** (on page 29).
Authorize DataMotion in the Sender Policy Framework.

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

Set Up Microsoft Office 365 for DataMotion SecureMail

This information describes how to set up Microsoft Office 365 to work with DataMotion SecureMail. (See the [Overview of the Setup](#) for a synopsis of the procedures.)

REVIEW THE REQUIREMENTS

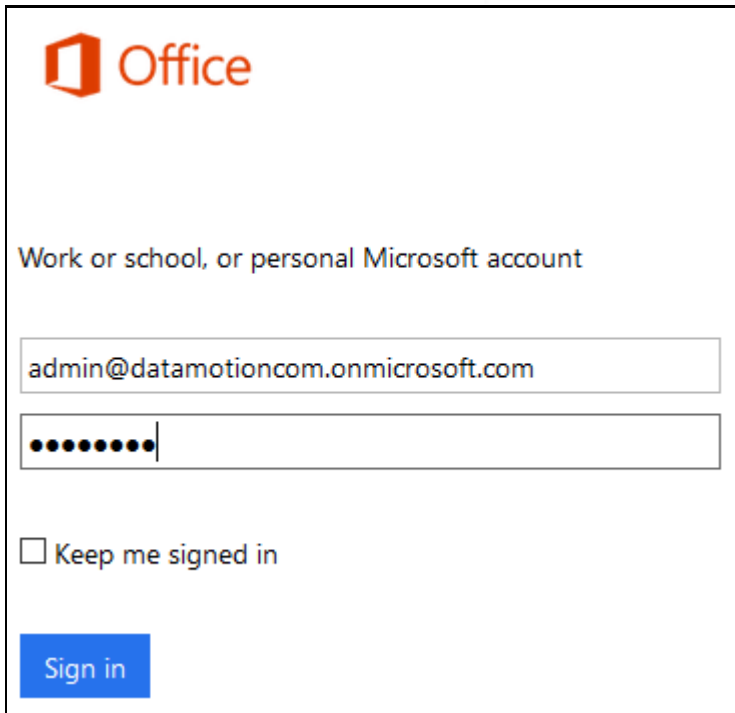
You must meet the following requirements to perform the DataMotion SecureMail setup for Office 365:

1. Your Office 365 setup must be complete, and Office 365 must be working.
2. You must have Office 365 administrative rights to perform the setup procedures in this guide.
3. You must have a DataMotion SecureMail account that has been provisioned and is ready to send secure emails.

SIGN IN TO OFFICE 365

Before performing the procedures in this guide, you must sign into Office 365 as an administrator.

1. Open a browser window and go to the Office 365 login page at <https://login.microsoftonline.com/>
2. Enter your credentials and click *Sign in*.



Office

Work or school, or personal Microsoft account

admin@datamotioncom.onmicrosoft.com

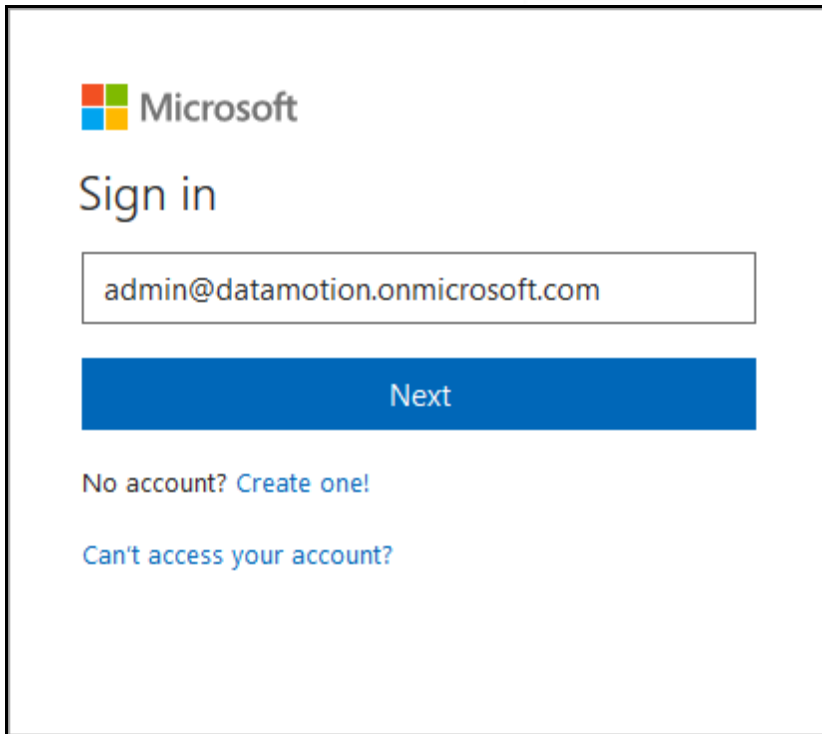
••••••••

Keep me signed in

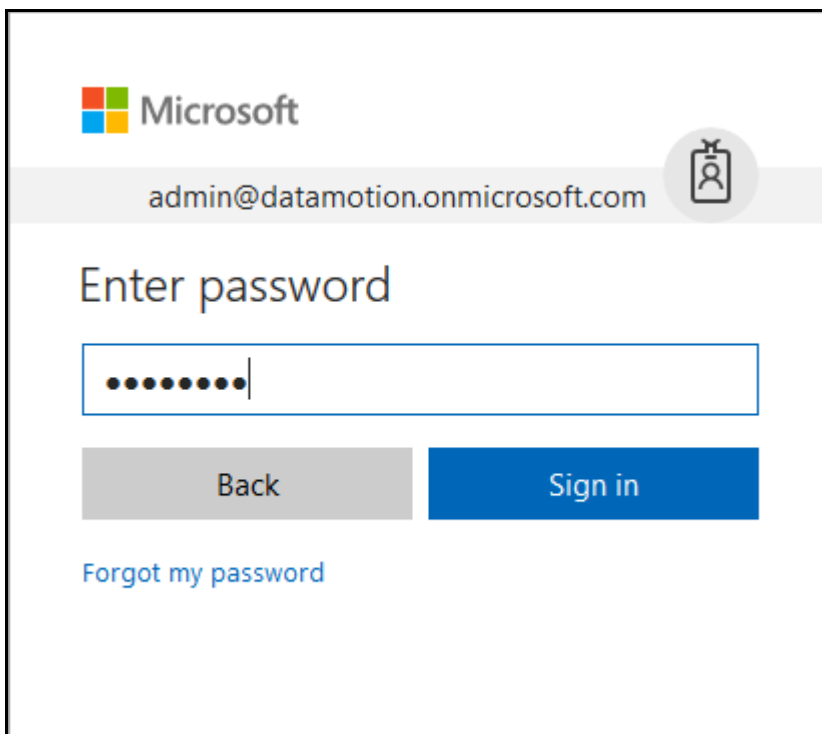
Sign in

NOTE: Depending on your sign-in experience you may see a different page entirely. If this is the case, use the instructions below:

1. Open a browser window and go to the Office 365 login page at <https://login.microsoftonline.com/>
2. Enter your Email or phone (if applicable).
3. Click Next.



4. Enter your password.
5. Click Sign in.

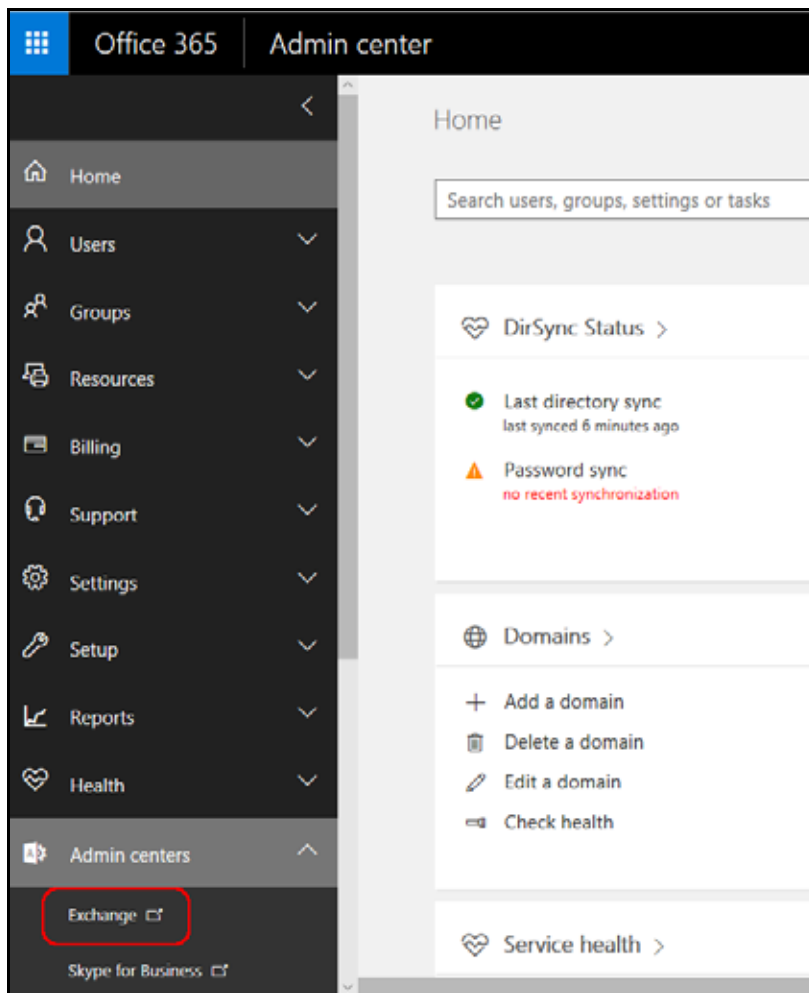


CREATE A CONNECTOR TO ROUTE EMAIL TO DATAMOTION SECUREMAIL

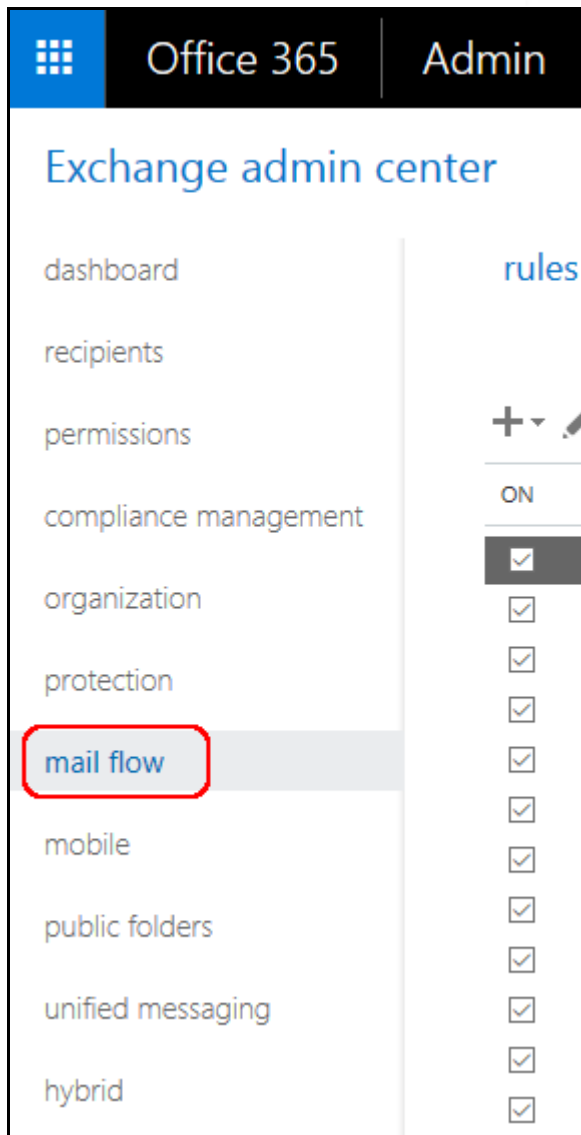
This procedure describes how to set up email routing to the DataMotion SecureMail gateway. This enables secure messages to be processed properly.

In the Microsoft Office 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 SecureMail smart host. (A smart host is a server that redirects outbound mail.) TLS ensures secure, encrypted routing to DataMotion.

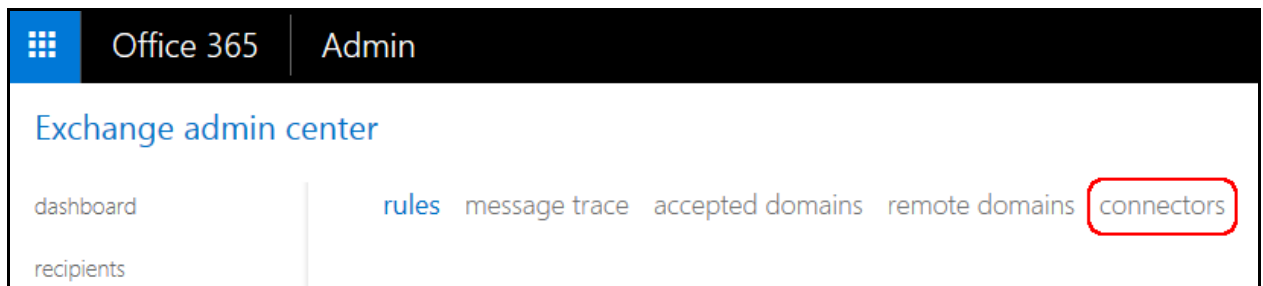
1. Under the Office 365 admin center pull out scroll down to the Admin centers section, and select **Exchange**.



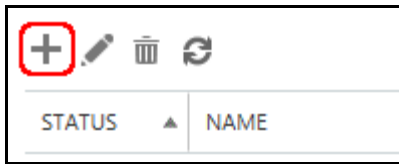
2. Click the **mail flow** section on the left side of the screen.



3. Click the **connectors** tab.



4. Select the **Plus icon (+)** to create a new connector. Refer to the example screen, and enter information as follows on the **Select your mail flow scenario** screen and all subsequent pages during this process:



- a. Select **Office 365** in the From: drop-down.
- b. Select **Partner organization** in the To: drop-down.
- c. Click **Next**.

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
[Learn more](#)

From:
 Office 365

To:
 Partner organization

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

- d. Type **DataMotion SecureMail** as the Name for the connector.
- e. Enter a description about what action the connector performs (see screenshot example).
- f. Click the Turn it on checkbox (optional but you will need to turn the connector on later).
- g. Click Next.

New connector

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

*Name:
DataMotion SecureMail

Description:
Route Message to DataMotion SecureMail server @ gateway.datamotion.com

What do you want to do after connector is saved?
 Turn it on

Next Cancel

- h. On the **When do you want to use this connector?** section select the **Only when I have a transport rule set up that redirects messages to this connector** radio button.
- i. Click Next.

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

Only when email messages are sent to these domains

+ ✎ -

Select this option only if you created a rule that redirects email messages to this connector.
[Learn more](#)

Back Next Cancel

- j. On the **How do you want to route email messages?** section select the **Route email through these smart hosts** radio button.
- k. Click the plus icon to add a smart host.
- l. In the textbox, type the following: **gateway.datamotion.com**
- m. 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

- n. The previous screen now contains the smart host you created.
- o. 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](#)

Use the MX record associated with the partner's domain

Route email through these smart hosts

+ ✎ -

gateway.datamotion.com

Back Next Cancel

- p. On the How should Office 365 connect to your partner organization's email server? section, ensure TLS checkbox is selected and the second radio button is chosen (see below for reference).
- q. Click Next.

New connector

How should Office 365 connect to your partner organization's 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

- r. A summary of all information entered during the process will be shown, review this information to ensure it matches these instructions (reference below) and then click Next.

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: Partner organization

Name
 DataMotion SecureMail

Description
 Route Message to DataMotion SecureMail server @ gateway.datamotion.com

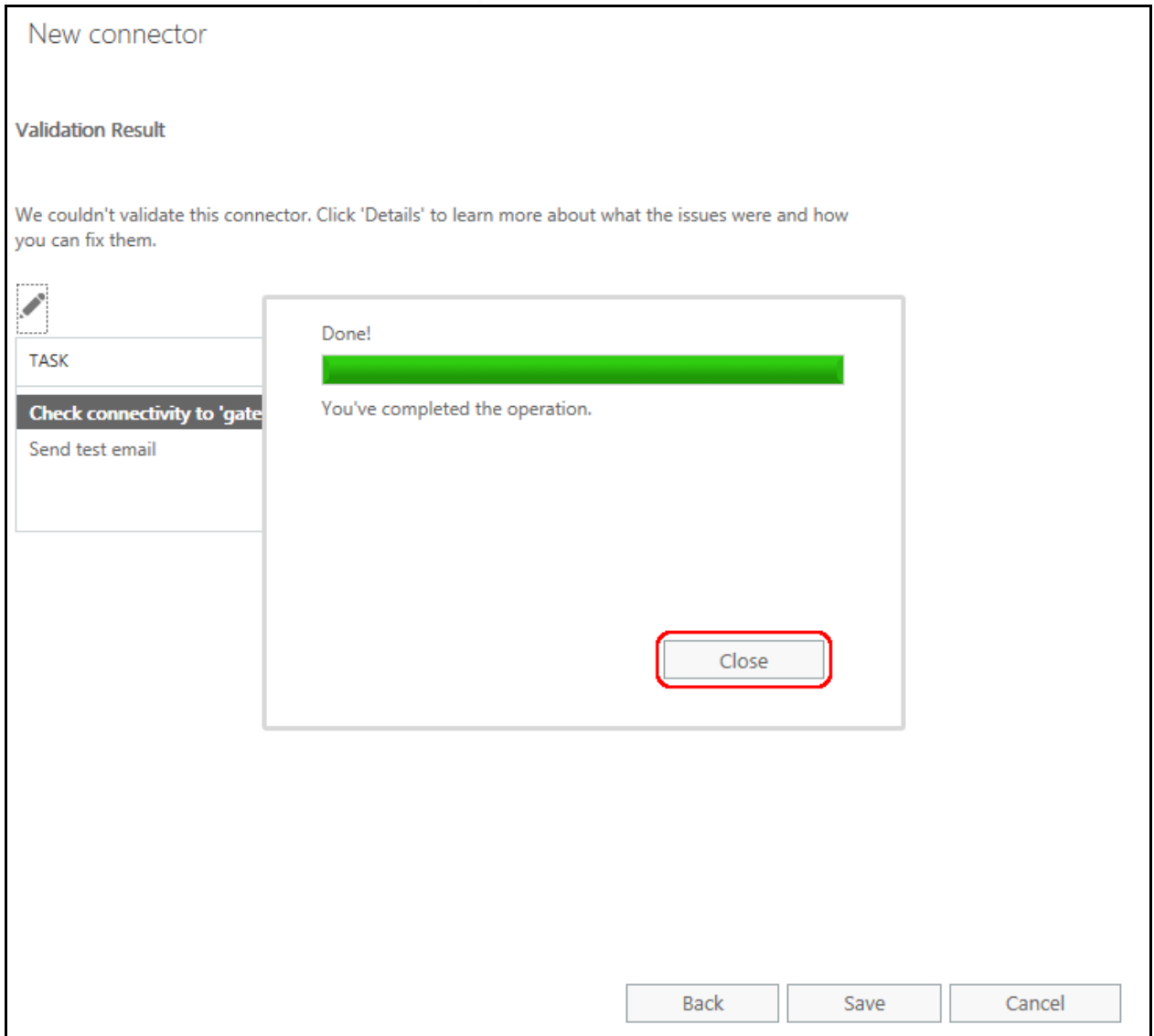
Status
 Turn it on after saving

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: gateway.datamotion.com

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).

- s. On the Validate this connector page you need to enter an email address to receive a test message. Click the plus icon to enter an address now.
- t. Enter an email of your choosing in the textbox and click OK.
- u. Click the Validate to button.
- v. When the process completes click the Close button in the pop-up window. You should have also received an email from Office 365 at the email you entered before clicking the Validate button.



w. Click the Save button to save the connector.

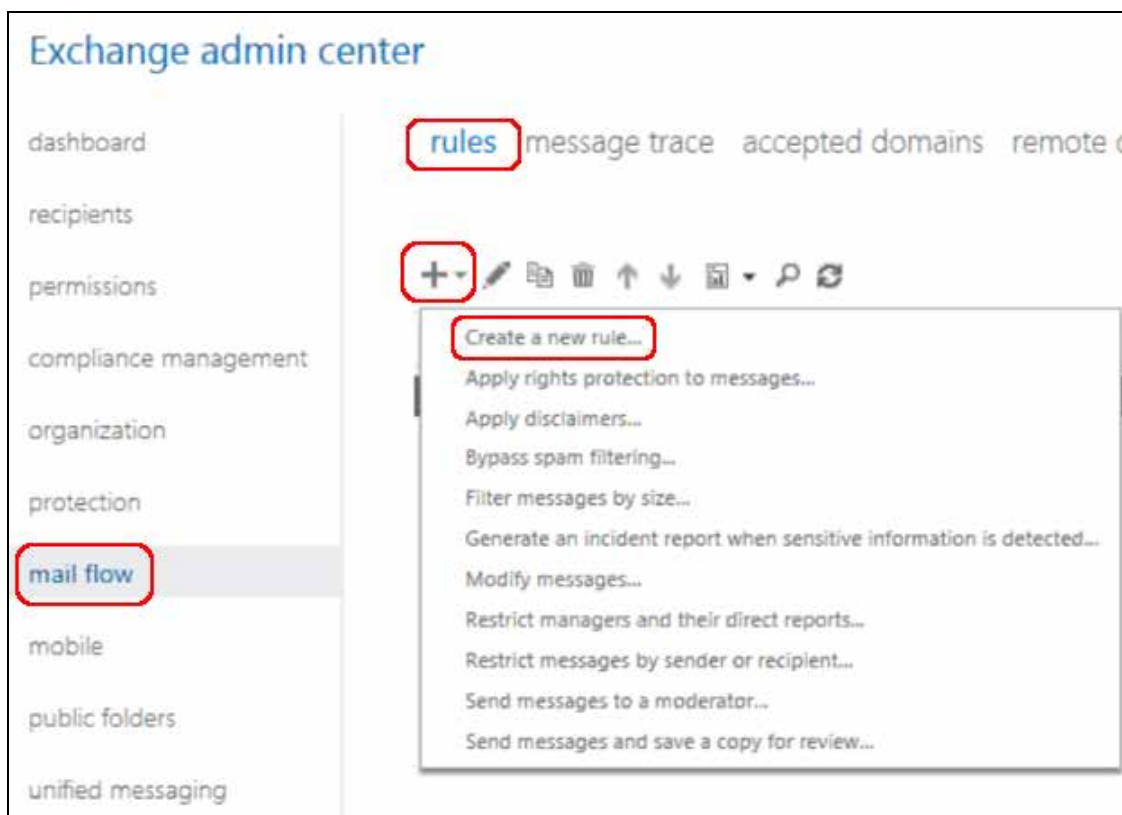
5. Turn the Connector On if you did not do so in the previous steps.

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 SecureMail Tag section.

USE MICROSOFT EXCHANGE TO CREATE A RULE WITH A SECUREMAIL TAG

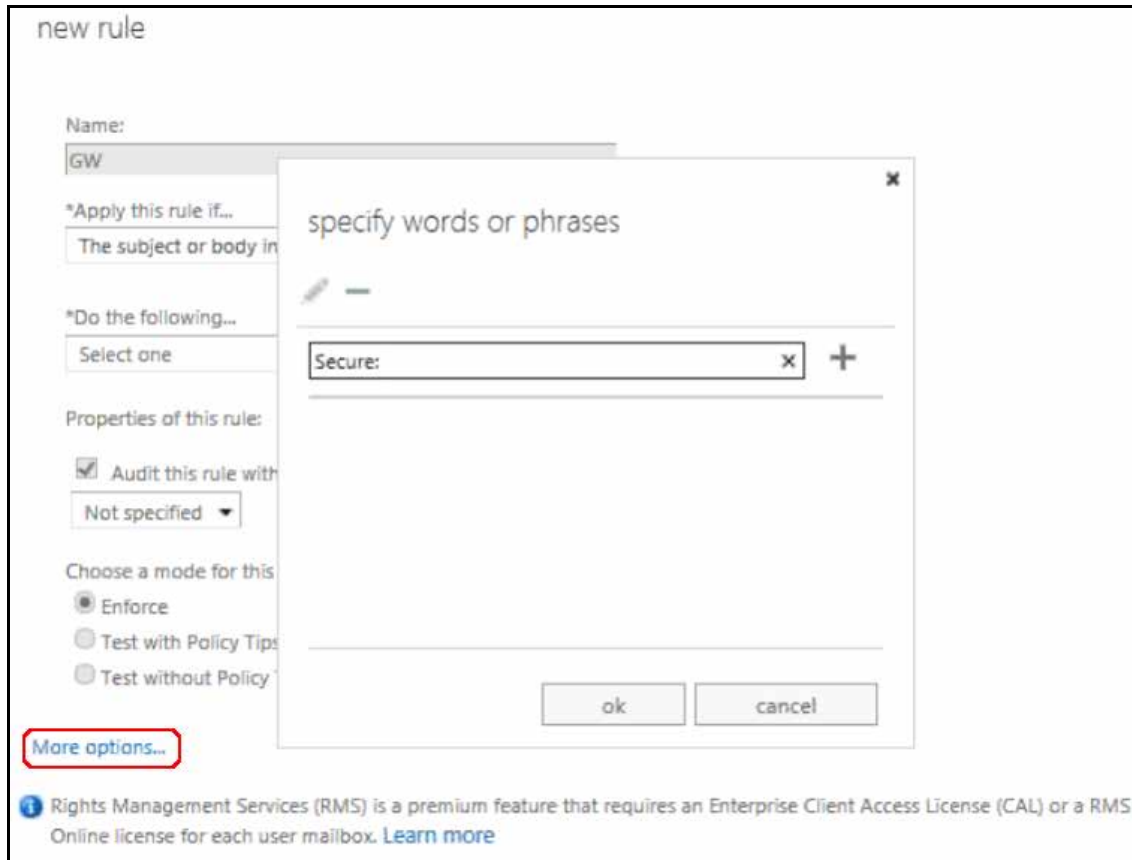
The following instructions describe setting up a Microsoft Office 365 mail flow rule to utilize the connector created in the Create a Connector to Route Email to DataMotion SecureMail section.

1. From your **Exchange Admin Center**:
 - a. Select **mail flow** from the menu on the left, and then select **rules** on the right.
 - b. Select the **Plus icon (+)** and then select **Create a new rule...**

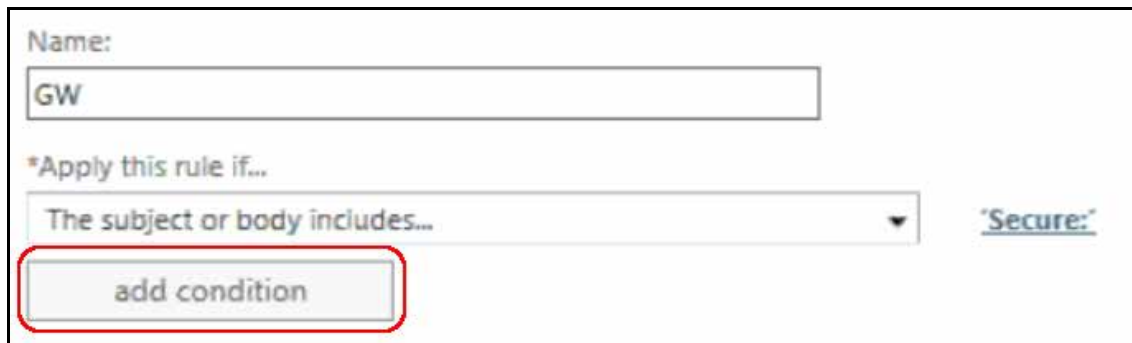


2. The following instructions involve setting up the new rule.
 - a. Add a **Name**. (In this example, we use “GW”.)
 - b. Click the drop-down field under **Apply this rule if...**
 - c. Point to **The subject or body includes...**
 - d. The Specify Words or Phrases dialog is displayed. In the entry 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 SecureMail server.
 - e. Click the **Plus icon (+)** to apply this text and then click OK.

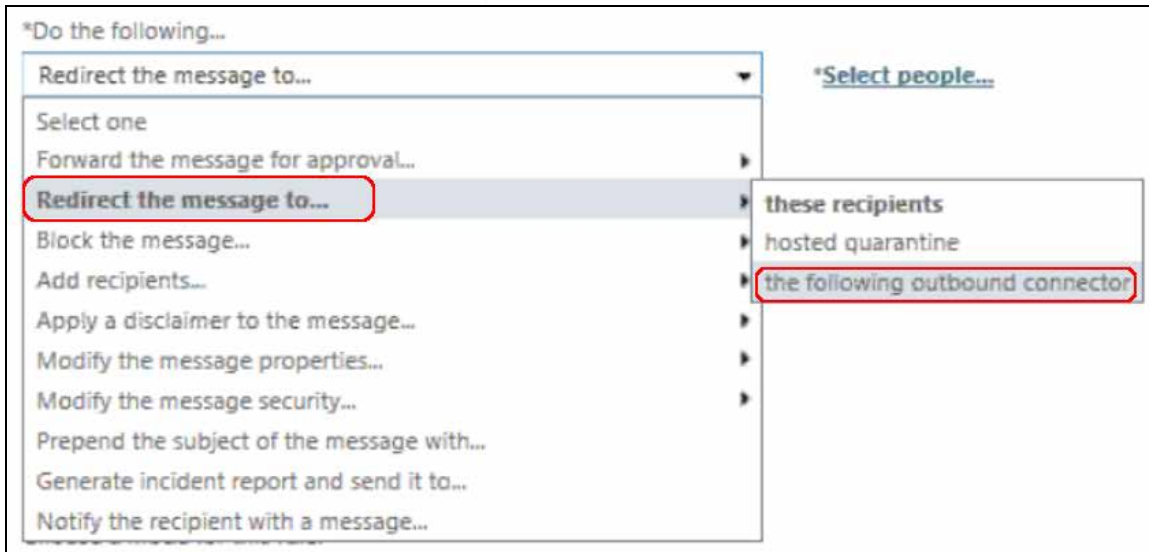
3. Click **More options...** to access the features for the next step.



4. To create the second condition for the rule, click **add condition** and follow the steps below.



5. Click the drop-down field under **Do the following...**
 - a. In the drop-down select **Redirect the message to...** and point to **the following outbound connector.**



b. In the popup window, select the DataMotion Outbound Connector that you previously created in the section *Create a Connector to Route Email to DataMotion SecureMail*, and click OK.

6. (Optional) add an exception to the rule for communication inside of the organization by first clicking **add action**.



- a. Click the drop-down field under **Except if...**
- b. Select **The recipient is located...** and point to **Inside the organization**.
- c. The exception should match the image below.



7. Click **Save**.

GW

GW

*Apply this rule if...

The subject or body includes... [Secure:](#)

add condition

*Do the following...

Use the following outbound connector... [DataMotion](#)

add action

Except if...

✖ The recipient is located... [Inside the organization](#)

add exception

Properties of this rule:

Priority:

0

Audit this rule with severity level:

Not specified

Choose a mode for this rule:

Enforce

Test with Policy Tips

Test without Policy Tips

Activate this rule on the following date:

Thu 2/26/2015 11:30 AM

Deactivate this rule on the following date:

Thu 2/26/2015 11:30 AM

Clear associated messages

save cancel

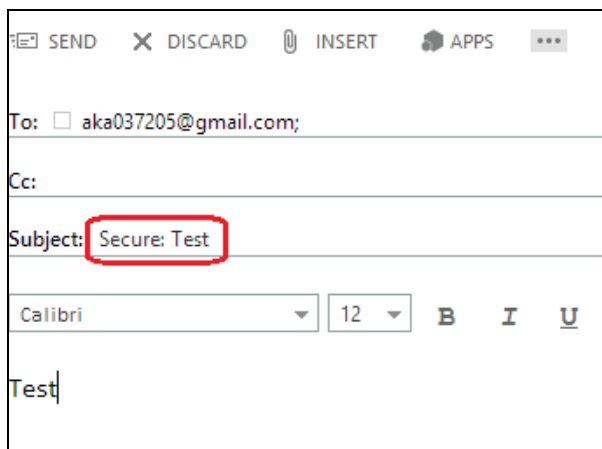
This completes the setup for adding the rule to the **mail flow**.

SEND A SECURE EMAIL (TO CONFIRM OPERATION)

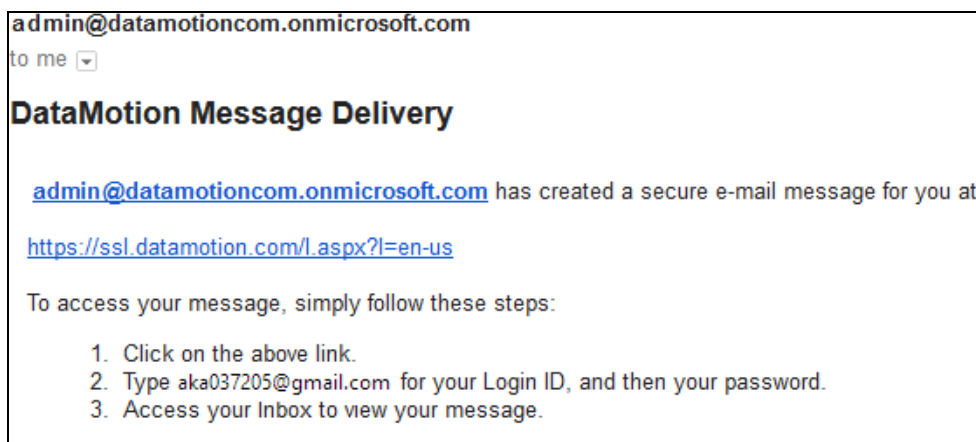
The following information illustrates how the Exchange rule works when sending a secure message.

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

1. From your Office 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 SecureMail message.)



2. Click **Send** to send the message. The recipient should then receive an email containing a SecureMail 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 SecureMail message, the recipient will create a new password for their account.

OPTIONAL: USE THE DATAMOTION SECUREMAIL PLUG-IN FOR MICROSOFT OUTLOOK

To simplify sending secure messages from Microsoft Outlook, DataMotion provides an Outlook plug-in (also known as “the SendSecure button”) that allows users to send secure emails with a single click of a button. The plug-in shows up as a special Send button on Microsoft Outlook. It is preconfigured to use a subject line tag of Secure: so when a user clicks on the button, a tag is automatically added to the subject line. The user does not have to enter a tag manually. Otherwise, everything works the same as described in [Send a Secure Email \(to Confirm Operation\)](#) on page 28.

Additional options and technical details related to the plug-in and its configuration are described in a separate document and are beyond the scope of this document. Please contact your DataMotion Sales representative for more information.

FINAL STEP: AUTHORIZE DATAMOTION AS AN EMAIL SENDER

To complete the setup, you must authorize DataMotion in the Sender Policy Framework.

A protocol called Sender Policy Framework (SPF) is used to protect against email spoofing (creation of email messages with a forged sender address where a third party sends emails posing as someone else).

Using SPF, the receiving mail server can validate if the sending server is authorized to send email on behalf of the sender. This can be done using SPF records that include a list of IP addresses authorized to send messages on behalf of the sender’s domain. If the IP address of the sending server is not found in that list, the email message can be flagged as spam or rejected by the receiving server.

It is important that you add the following SPF record to your external DNS configuration so that the DataMotion secure email server will be identified as an authorized email sender on behalf of your organization:

```
IN TXT: v=spf1 a ip4:20.42.36.97 -all
```

Note: You will need to have access to your external DNS server record to do this. If you do not manage your DNS directly, please provide this information to your DNS administrator.

For more information on SPF records, see the SPF Project’s article on “Introduction to Sender Policy Framework” at www.openspf.org/Introduction.

4

Additional Technical Information

Refer to the following for important technical information.

DATAMOTION IP WHITELIST FOR MICROSOFT OFFICE 365

DataMotion currently whitelists the following Microsoft Office 365 outbound SMTP servers to ensure proper communication between servers.

65.55.88.0/24	65.55.88.1	65.55.88.254	255.255.255.0
207.46.51.64/26	207.46.51.65	207.46.51.126	255.255.255.192
207.46.163.0/24	207.46.163.1	207.46.163.254	255.255.255.0
213.199.154.0/24	213.199.154.1	213.199.154.254	255.255.255.0
213.199.180.128/26	213.199.180.129	213.199.180.190	255.255.255.192
216.32.180.0/24	216.32.180.1	216.32.180.254	255.255.255.0
216.32.181.0/24	216.32.181.1	216.32.181.254	255.255.255.0

NOTE: For additional technical and user documentation available from DataMotion, see [DataMotion Documentation](#) (on page 8).

* * *

This represents the end of the *DataMotion SecureMail Setup Guide for Microsoft Office 365*.