



DataMotion SecureMail G Suite Setup Guide

July 28, 2021
Part # 050014-05

Copyright © 2008 - 2021, 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 for G Suite™ Service Setup Guide v5

Publication Date: July 28, 2021

Printed in the United States of America.

DataMotion, Inc. Confidential and Proprietary Information.

Published By:

DataMotion, Inc.
200 Park Ave., Suite 302
Florham Park, NJ 07932
USA

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

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

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY	6
----------------------------	----------

DATAMOTION SECUREMAIL FOR G SUITE™	6
---	----------

2 GETTING STARTED	7
--------------------------	----------

INITIAL SETUP FOR G SUITE	7
AUTHORIZING DATAMOTION	7

3 GMAIL SETTINGS	9
-------------------------	----------

ACCESSING THE GMAIL SETTINGS	9
ADDING A MAIL HOST	12
CONTENT COMPLIANCE SETTINGS	14

4 ADDITIONAL INFORMATION	20
---------------------------------	-----------

GOOGLE DOCUMENTATION	20
DATAMOTION DOCUMENTATION	20

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: *Gmail Settings*

- Changed all screenshot and instructional information to match new G-Suite UI in sections *Accessing the Gmail Settings*, *Adding a Mail Host*, and *Content Compliance Settings*

Version 4

Chapter 2: *Getting Started*

- Changed the SPF record to match the new IP from Azure.

Version 3

All references to Google Apps have been altered to G Suite reference the Google re-brand of Google Apps to G Suite.

Chapter 3: *Gmail Settings*

- Changed most screenshots and the corresponding instructions in this section to reflect the changes made to Google Apps Administration.

Version 2

Chapter 2: *Getting Started*

- Added a new section on *Initial Setup for G Suite* (on page 7)
 - » Describes the installation of Google Apps.
- *Accessing the Gmail Settings* (on page 9)
 - » Replaced most screenshots to reflect the new Administrator interface in Google Apps.

Chapter 3: *Gmail Settings*

- *Content Compliance Settings*: (on page 14):
 - » Changed instructions for the Add Setting popup to state that a description is now a required field instead of an optional one.
 - » Screenshot changes to better reflect the new interface were also added for most of the screens.

Version 1

The initial version of this document.

1

Executive Summary

DATAMOTION SECUREMAIL FOR G SUITE™

The DataMotion SecureMail for G Suite™ service allows sensitive data to be securely exchanged with customers, business partners and vendors. It's easy to use since SecureMail integrates with applications, mobile devices and systems already in use, without the need to install special apps or exchange encryption keys. After following the steps in this guide, G Suite for Business, Education, or Government customer can send and receive sensitive data right from their Gmail™ webmail service, with confidence that the messages are delivered securely and in compliance with privacy regulations.

2

Getting Started

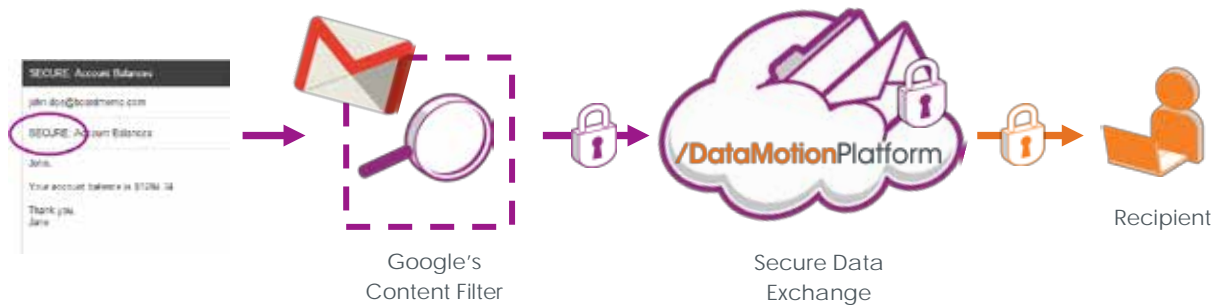
INITIAL SETUP FOR G SUITE

To setup SecureMail for your Gmail accounts, you must first setup a valid G Suite for Business account. A domain owned by your company is also necessary for the G Suite for Business setup and to fully integrate DataMotion SecureMail. A technical administrator with access to DNS management and has familiarity with G Suite setup is highly recommended for completing these steps and all steps going forward in this guide.

AUTHORIZING DATAMOTION

A protocol called Sender Policy Framework (SPF) has been developed in order to protect against email spoofing (creation of email messages with a forged sender address where a 3rd party sends emails posing as someone else).

Using SPF, the receiving mail server can validate if the sending server is authorized to send on the sender's behalf. This is done using the 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 even rejected by the receiving server.



To prevent this scenario from happening, it is important to add the following SPF record for the DataMotion mail server in your DNS configuration as an authorized email sender on your behalf.

```
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.

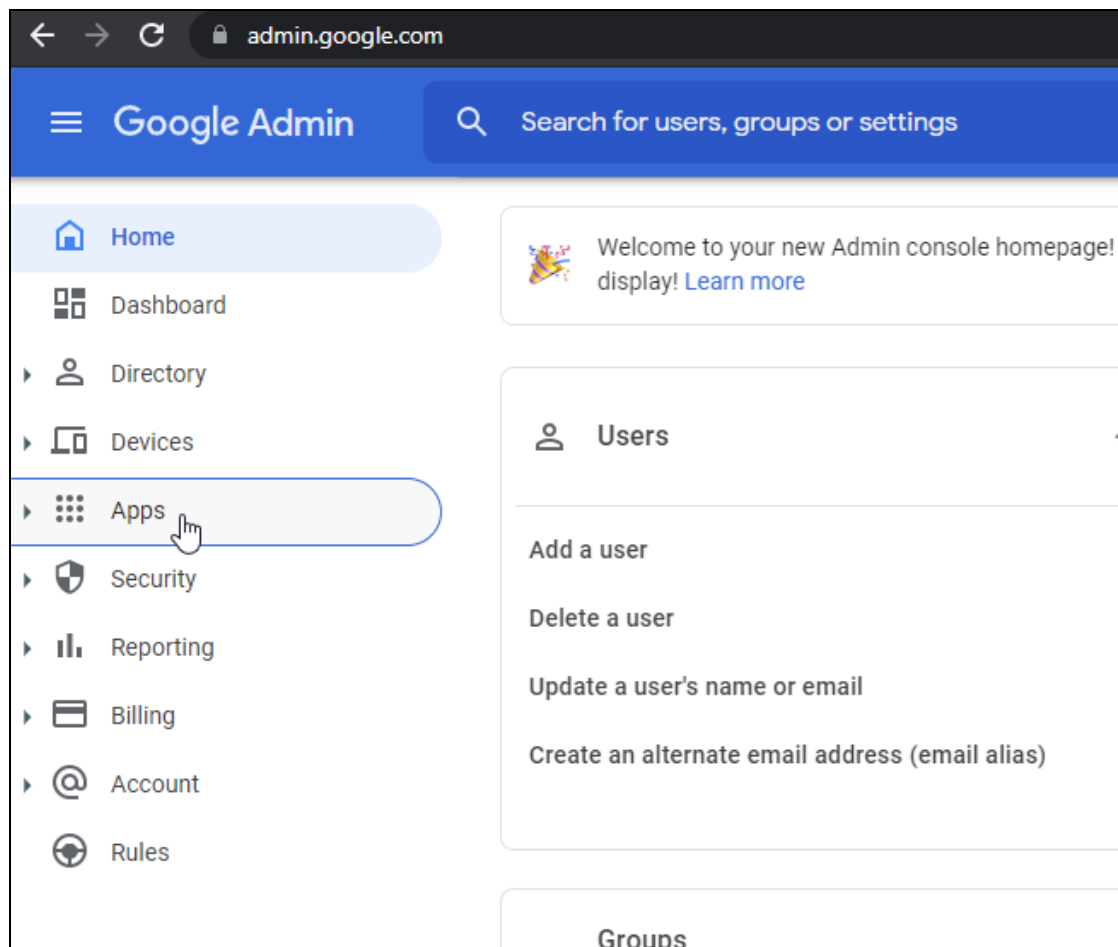
For more information about SPF Records, see The SPF Project's [Introduction to Sender Policy Framework](#).

For more information, see [DataMotion Documentation](#) on page 20

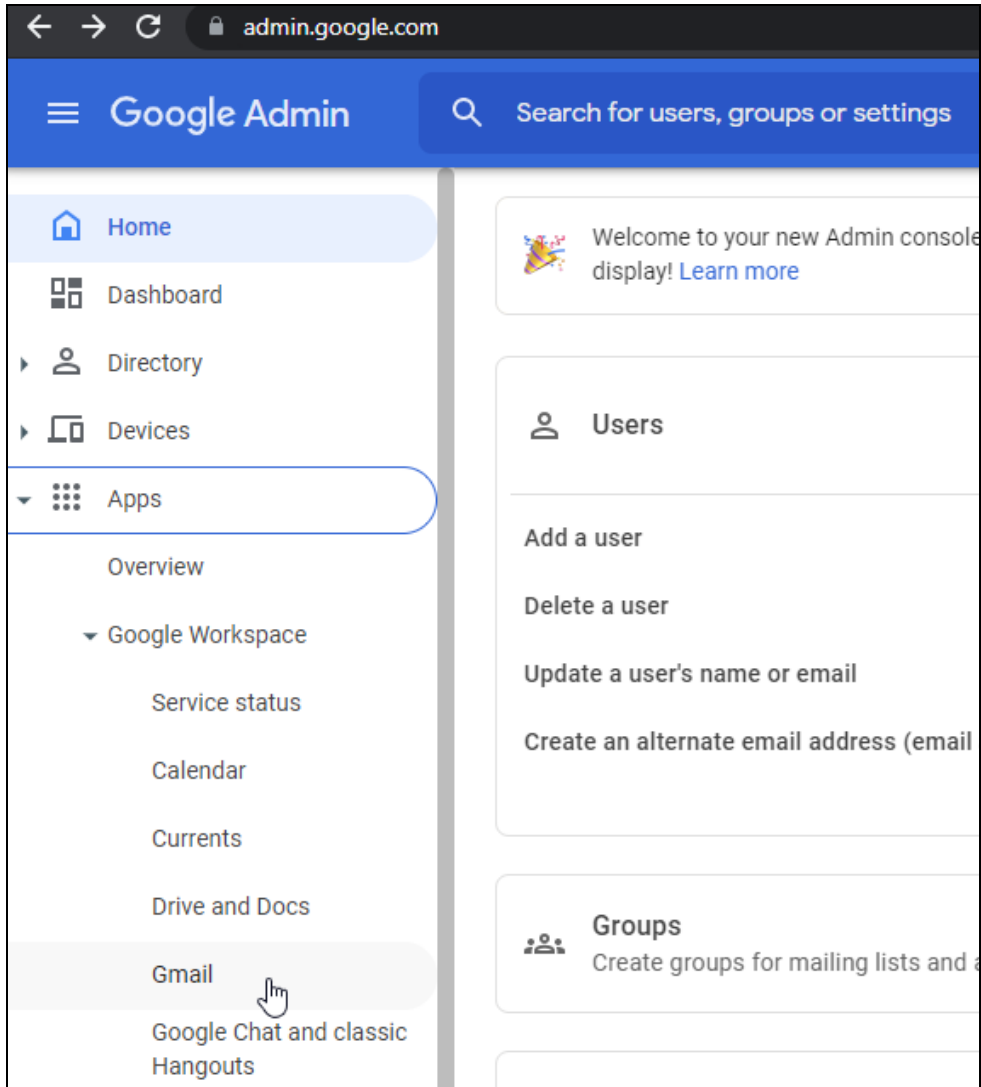
3 Gmail Settings

ACCESSING THE GMAIL SETTINGS

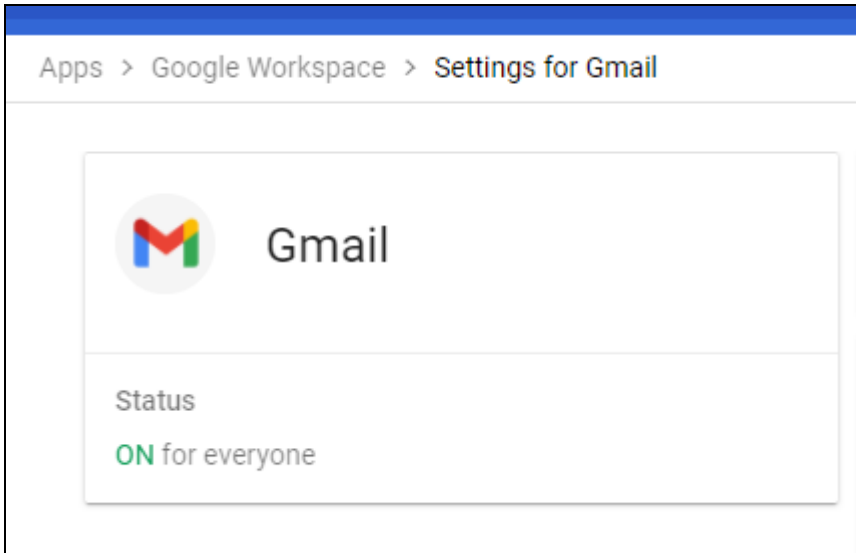
1. Log in to the **G Suite** at: <https://admin.google.com>.
2. Click on **Apps** dropdown.



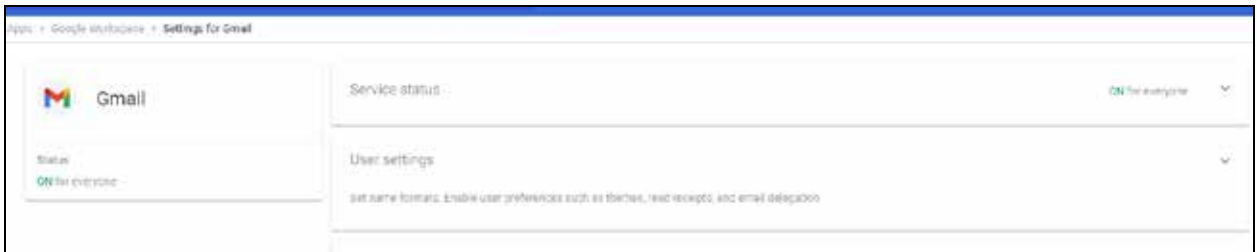
3. Click on **Gmail**.



4. Make sure **Gmail** is turned **On for everyone**.



As shown above, you should be on the Settings for Gmail page which is where the next set of steps need to take place.



Please see [below](#) for the next steps.

ADDING A MAIL HOST

1. On the **Settings for Gmail** page, click on the **Hosts** dropdown.



2. Select **Add route** to create a mail route to the DataMotion SecureMail Gateway.
3. Use the following settings for the mail route.
 - » Name: **DataMotion**
 - » Select **Single Host** email server
 - » Host Name: **gateway.datamotion.com**
 - » Port: **587**
 - » Select **Require secure transport (TLS) connection (Recommended)**
 - » Select **Require CA signed certificate (Recommended)**
 - » Select **Validate certificate hostname (Recommended)**
 - » Click Test TLS connection
4. Select **Save** to create the route.

Add mail route

Name [Learn more](#)

DataMotion

This field is required.

1. Specify email server

Only ports numbered 25, 587, and 1024 through 65535 are allowed.

Single host ▾

gateway.datamotion.c : 587

2. Options

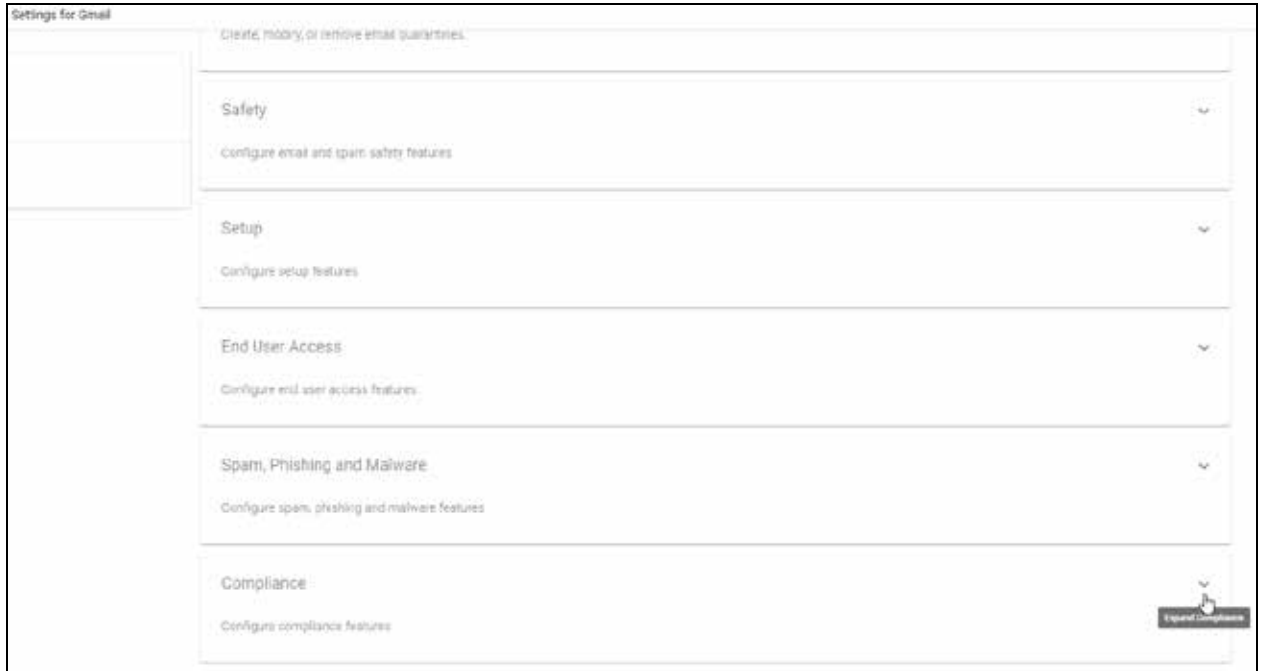
- Perform MX lookup on host
- Require mail to be transmitted via a secure (TLS) connection (Recommended)
- Require CA signed certificate (Recommended)
- Validate certificate hostname (Recommended)

[Test TLS connection](#) TLS connection validated on July 28, 2021 2:38 PM

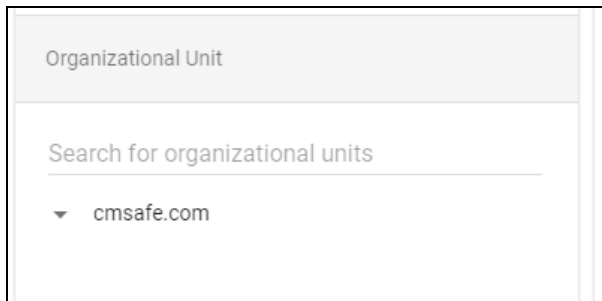
CANCEL **SAVE**

CONTENT COMPLIANCE SETTINGS

1. Back on the **Settings for Gmail** page, scroll down and click on the **Compliance** drop down.



2. In the **Organizational Unit** section, highlight your domain or the OU for which you want to configure settings.



3. Scroll to the **Content compliance** section and select **Configure** or **ADD ANOTHER RULE** if you already have rules in place.

Description	Status	Source	Actions	ID	Messages	Matches	Consequences
SecureMail	Enabled	Locally applied	Edit - Disable - Delete	8beaf	Outbound Internal - sending	1	Modify message Change route
SF-Sandbox	Enabled	Locally applied	Edit - Disable - Delete	79d51	Outbound Internal - sending	1	Modify message Change route
Sandbox Safe TLS	Enabled	Locally applied	Edit - Disable - Delete	180dc	Outbound Internal - sending	1	Modify message Change route
SecureMail SAFETLS	Enabled	Locally applied	Edit - Disable - Delete	8c6a5	Outbound Internal - sending	1	Modify message Change route

[ADD ANOTHER RULE](#)

- In the **Add setting** pop-up window, select **Outbound** and **Internal – sending** to ensure that all outbound messages are affected by this rule. Add “SecureMail” (or other appropriate description) to proceed.

Add setting

Content compliance [Learn more](#)

SecureMail

1. Email messages to affect

Inbound

Outbound

Internal - Sending

Internal - Receiving

- Select **Add** in the **Expressions** section.

2. Add expressions that describe the content you want to search for in each message

If ANY of the following match the message ▼

Expressions

No expressions added yet. [Add](#)

ADD

- » Select **Advanced content match**
- » Set the Location to **Subject**

- » Set the Match type to **Starts with**
- » Set Content to a subject tag, “SECURE” for this tag will be used to identify messages that will be routed to the DataMotion mail host for secure delivery to your recipient.

NOTE: The tag set here must be matched exactly for each secure message.

6. Select **Save**.

The screenshot shows a dialog box titled "Add setting". It has a blue header bar. Below the header, there is a section titled "Advanced content match" with a dropdown arrow. Underneath, there are three rows of settings, each with a label and a dropdown arrow:

- Location: Subject
- Match type: Starts with
- Match type: Contains text

Below these settings is a text input field labeled "Content" containing the text "SECURE". At the bottom right of the dialog, there are two buttons: "CANCEL" and "SAVE". A mouse cursor is pointing at the "SAVE" button.

7. You must set an action for the **3. If the above expressions match, do the following** section select **Change route** and select the DataMotion mail host you created in the section on [Adding a Mail Host](#).

Add setting

3. If the above expressions match, do the following

Modify message ▾

Headers

- Add X-Gm-Original-To header
- Add X-Gm-Spam and X-Gm-Phishy headers
- Add custom headers

Subject

- Prepend custom subject

Route

- Change route
- Also reroute spam
- Suppress bounces from this recipient

DataMotion ▾

8. In the **Show options** section select the account types to effect and any other options desired.
9. Select **Save** on the Advanced settings screen at the bottom of the page when it appears.

Add setting

Add more recipients

Encryption (onward delivery only)

Require secure transport (TLS)

[Hide options](#)

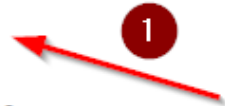
A. Address lists

Use address lists to bypass or control application of this setting

Bypass this setting for specific addresses / domains

Only apply this setting for specific addresses / domains

B. Account types to affect

Users 


Groups

Unrecognized / Catch-all

C. Envelope filter

Only affect specific envelope senders

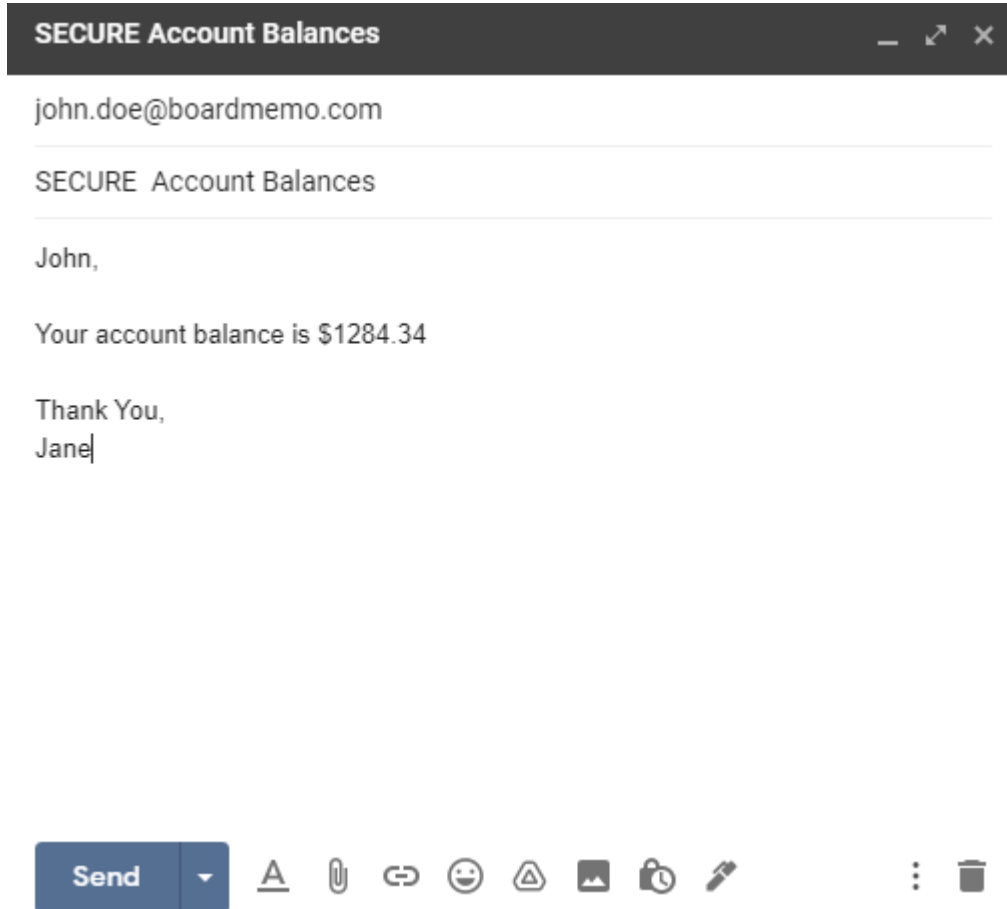
Only affect specific envelope recipients



CANCEL SAVE

NOTE: Changes made to the Content Compliance settings may require at least an hour to take effect.

Congratulations! You've successfully integrated the DataMotion platform into your G Suite environment. Any user account listed in your organization will be able to send secure messages by simply tagging a secure message with the secure tag expression.



4

Additional Information

GOOGLE DOCUMENTATION

- n [Enabling/Disabling Services](#): Administrators have the ability to control user access to specific applications. For detailed instructions on how to turn services on or off, see [Turn on or off G Suite services](#).
- n [Content Compliance Setting](#): There are many options when configuring the expressions used to route messages to DataMotion. For detailed descriptions about each of the options, see [Content compliance setting](#).
- n [Regex Examples](#): The Content Compliance settings also accepts regular expressions, or regex, to match patterns of text, rather than words or phrases. For guidelines and examples of the RE2 Syntax that Google uses, see [Examples of Regular Expressions](#).

DATAMOTION DOCUMENTATION

- n [SPF Records](#): For more information about SPF Records, see The SPF Project's [Introduction to Sender Policy Framework](#).
- n [IP Whitelist](#): DataMotion currently whitelists the following IP addresses for Google's outbound SMTP servers to ensure proper communication between servers:

```
ip4:216.239.32.0/19
ip4:64.233.160.0/19
ip4:66.249.80.0/20
ip4:72.14.192.0/18
ip4:209.85.128.0/17
ip4:66.102.0.0/20
ip4:74.125.0.0/16
ip4:64.18.0.0/20
ip4:207.126.144.0/20
ip4:173.194.0.0/16
```

If you are currently using an IP address that is not listed above, please contact us.