FortiMail Cloud Integration with Microsoft 365 Deployment Guide

Version 1.0





FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

https://cookbook.fortinet.com

FORTINET TRAINING SERVICES

https://www.fortinet.com/training

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com



April 27, 2022

TABLE OF CONTENTS

Change Log 4
Introduction 5
Configuring Domains on MS365 6
Configuring DNS Settings 7
Configuring Inbound Settings on FortiMail 8
Configuring Inbound Settings on MS365 9
  Configuring Inbound Transport Rule on MS365 9
Configuring Outbound Settings on FortiMail 12
Configuring Outbound Settings on Office 365 13
  Configuring Outbound Connector on MS365 13
  Configuring Outbound Transport Rule on MS365 15

Change Log

Date	Change Description
2022-01-13	Initial release.
2022-09-16	Bug fixes.

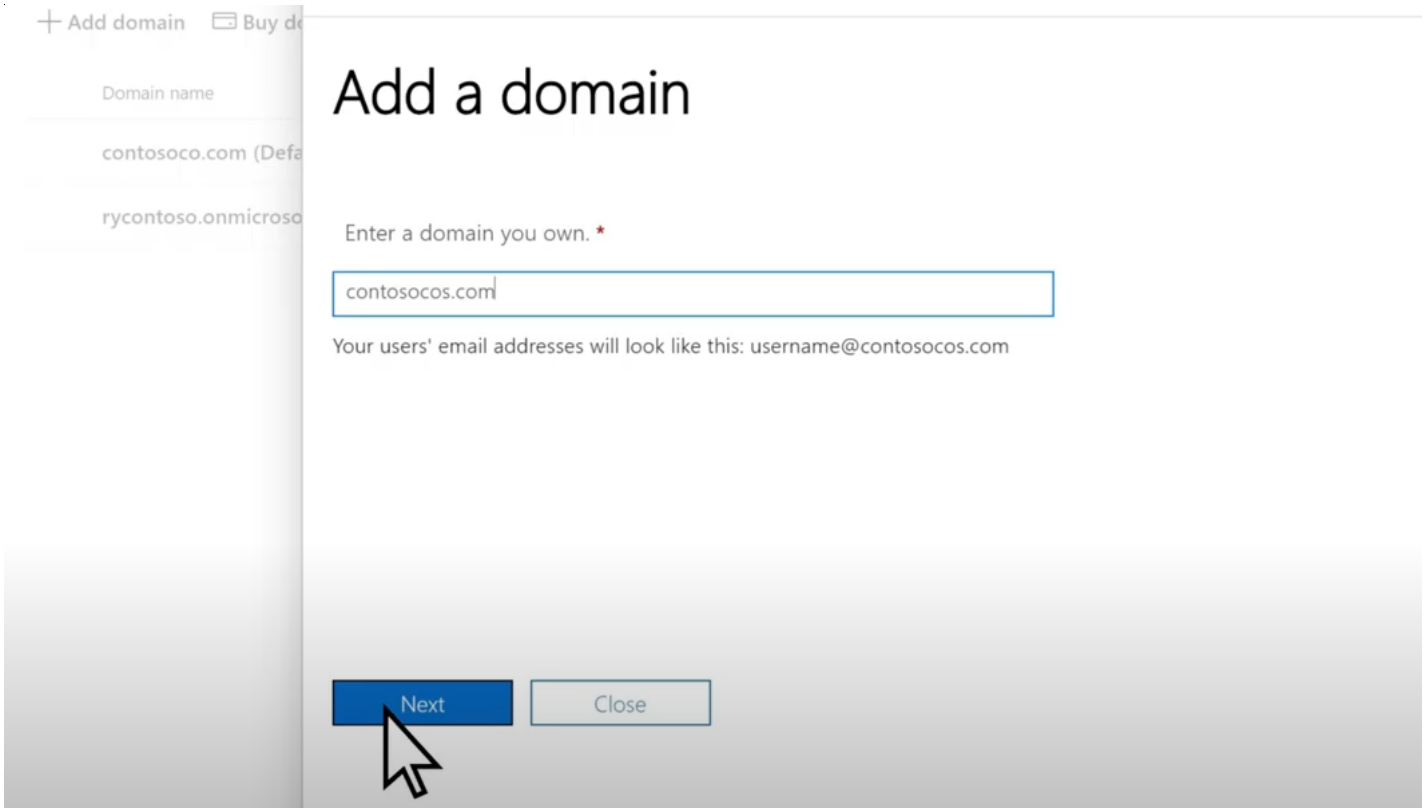
Introduction

This document outlines the basic configuration steps required to integrate FortiMail Cloud with Microsoft Exchange Online (Microsoft 365) so that FortiMail can scan and protect inbound and outbound email to and from MS365.

.

Configuring Domains on MS365

1. Log on to the MS365 admin center: https://admin.exchange.microsoft.com/#/homepage.
2. Select *Setup*.
3. Under *Get your custom domain set up*, select *View*.
4. Select *Manage*, and then *Add domain*.
5. Enter the new domain name, then select *Next*.

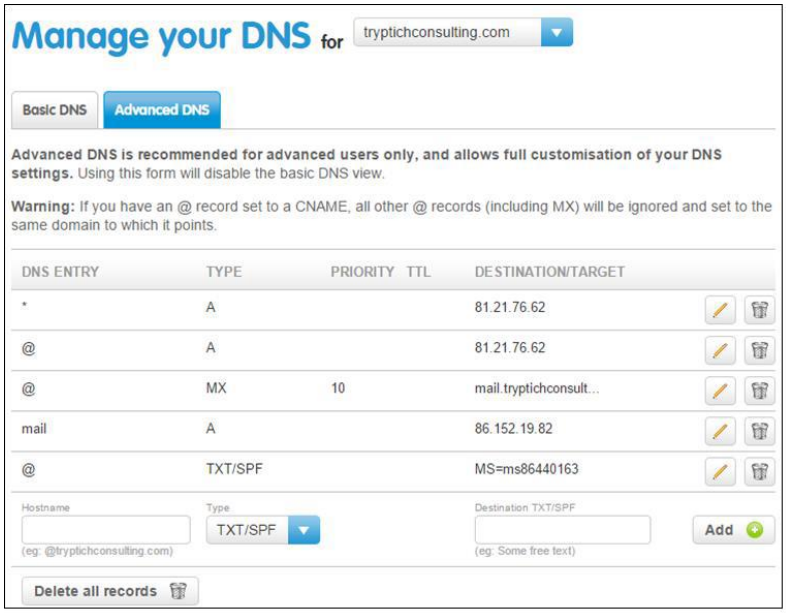


6. Log on to your domain registrar, in this case, GoDaddy, and select *Next*.
7. If prompted, log on to your registrar, and select *Authorize*.
8. Select *Add the DNS records for me*, and select *Next*.
9. Select the services for your new domain and clear the check boxes for any services that will be handled by a different domain. For example, if you just want to use the new domain for email, choose *Exchange*, and clear the check boxes for *Skype for Business* and *Mobile Device Management for Office 365*.
10. Select *Next*, then *Finish*. Your new domain has been added.

For more information about MS365 domain configuration, see https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide.

Configuring DNS Settings

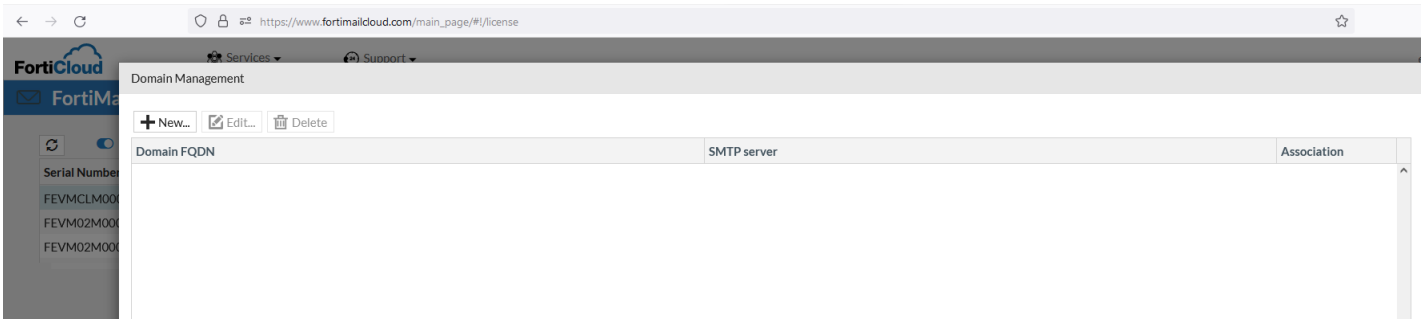
1. Log on to your DNS server.
2. Change the MX record from MS365 to FortiMail.



Configuring Inbound Settings on FortiMail

You will now configure the FortiMail cloud to accept mail from your domain and then forward the mail to Office 365.

1. Go to FortiMail Cloud user portal: https://www.fortimailcloud.com/main_page.
2. Select the FortiMail instance.
3. Select *Action* > *Manage Domain*.
4. Click *New*, and add the domain by entering the domain name and the SMTP server.

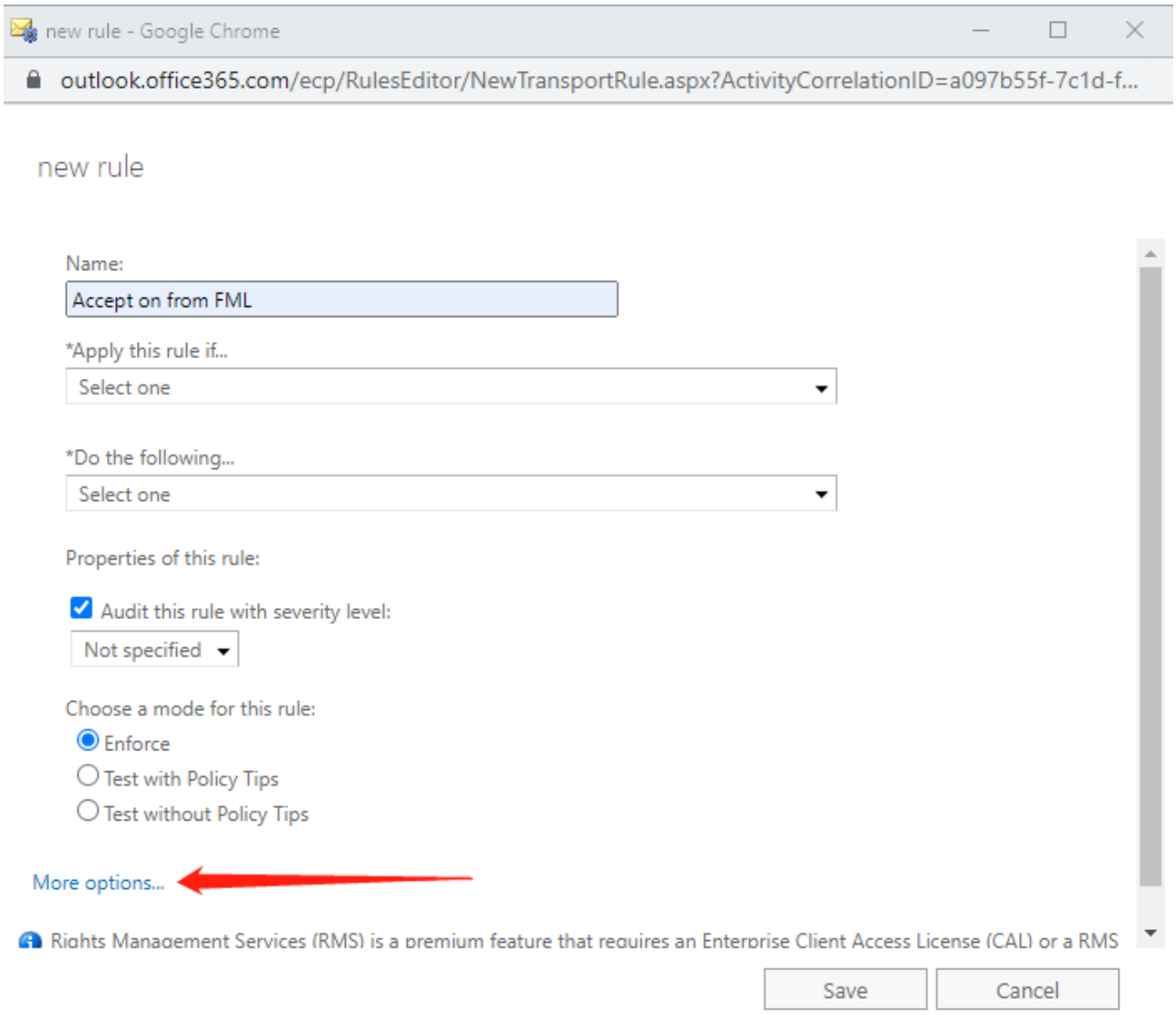


Configuring Inbound Settings on MS365

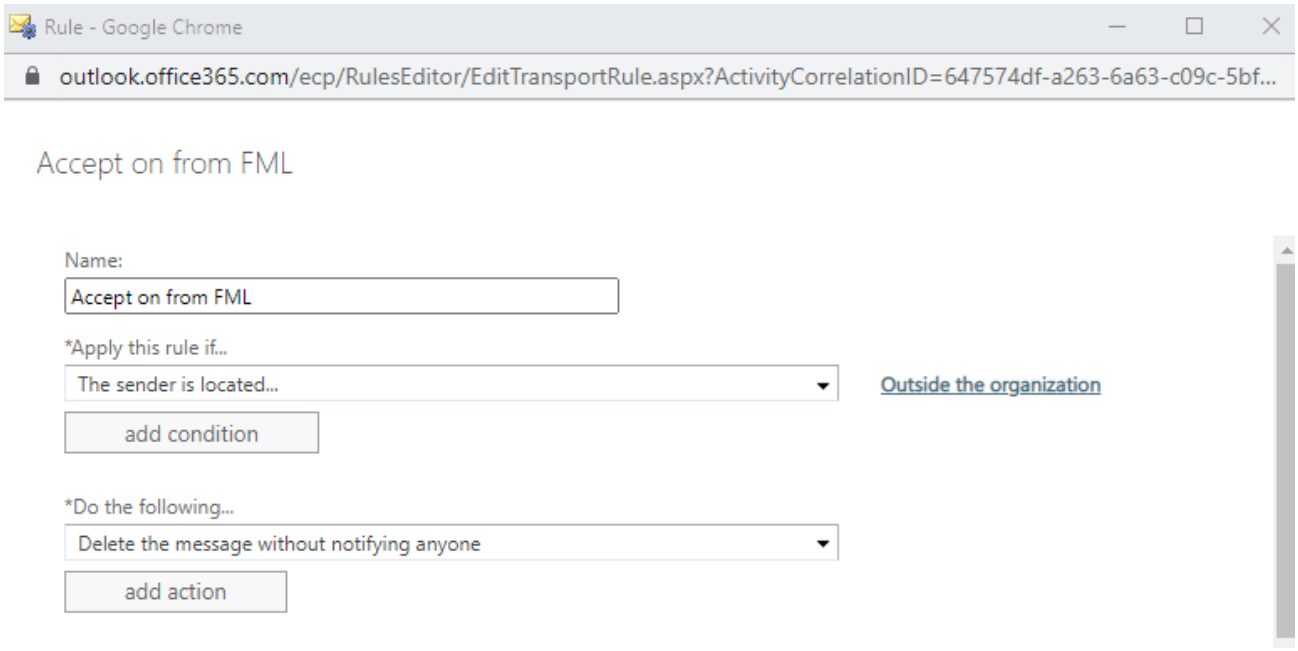
Now you'll configure MS365 to accept inbound email from FortiMail Cloud once the email has been scanned.

Configuring Inbound Transport Rule on MS365

1. Log on to the Exchange admin center: https://admin.exchange.microsoft.com/#/homepage.
2. Select *Mail Flow*.
3. Select the plus sign (+) dropdown menu and select *Create a new rule…*
4. Enter a name for the new rule.
5. Select *More options*.



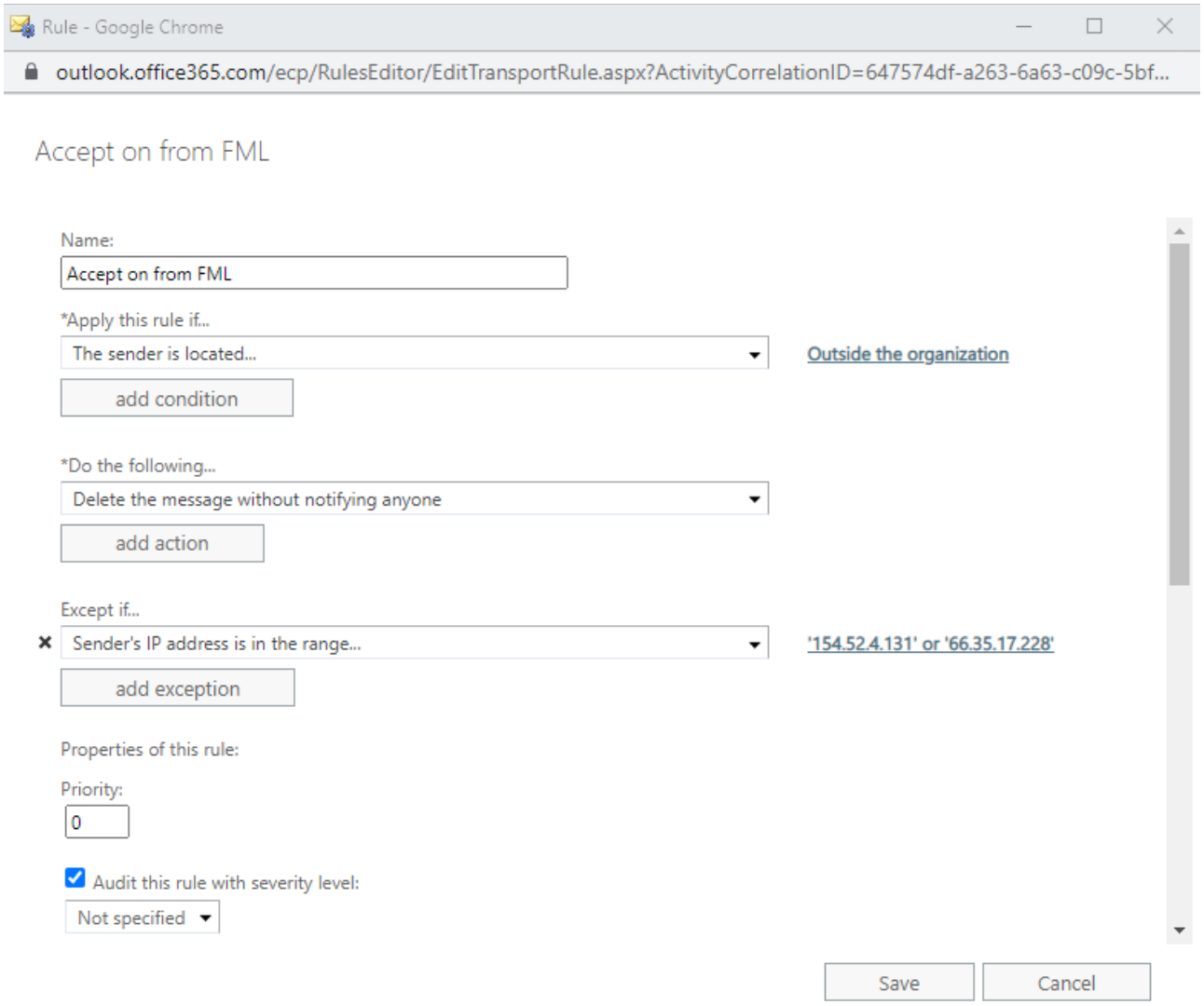
6. Edit *Apply this rule if* and *Do the following* as shown in the following example.



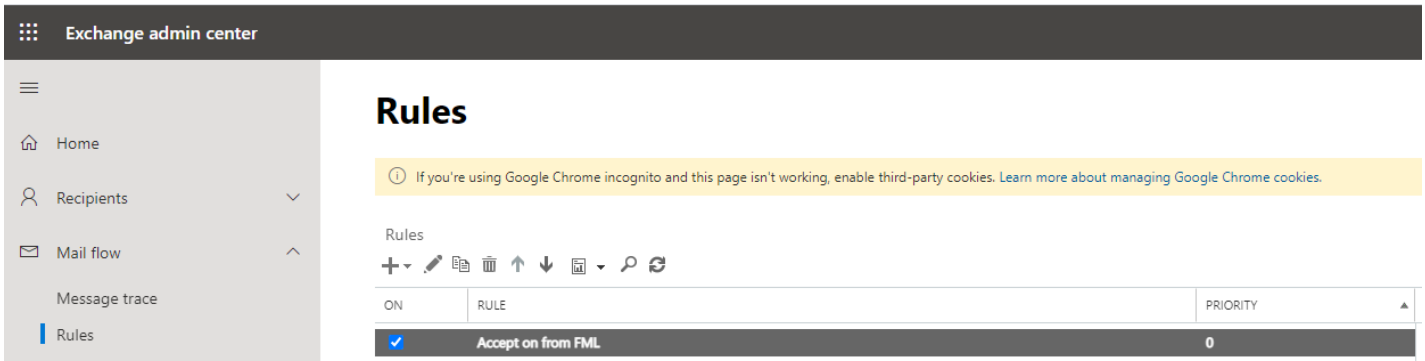
7. Edit *Except if* and enter the IP address based on your FortiMail Cloud instance.
   For example, if the hostname is example-com.fortimailcould.com, the IP address you need to enter should be the IP address of example-com.fortimailcould.com

```
#dig example-com.fortimailcould.com

;; ANSWER SECTION:
example-com.fortimailcloud.com. 3600 IN A 66.35.17.228
example-com.fortimailcloud.com. 3600 IN A 154.52.4.131
```



8. Configure a new rule to drop all inbound mail, unless it comes from FortiMail Cloud and select the *Accept only from FML* checkbox in the *ON* column under the rules section of the *Exchange admin center*.



Configuring Outbound Settings on FortiMail

Now that you have configured the inbound mail settings on both MS365 and FortiMail, you will need to configure your ACL policies on FortiMail. The “allow” relay policies will permit MS365 sources to relay outbound messages to external domains via FortiMail.

The ACL policy is pre-configured in the provisioning process if you enter MS365 as the server type in your provision template. You may verify it in your FortiMail Cloud instance.

If the ACL policy is not configured, follow the steps below to set it up.

1. Open the FortiMail CLI Console.
2. Enter the following commands:

```
config policy access-control receive
     edit 1
          set sender-ip mask 23.103.132.0/22 <this is your MS365
     server IP address>
          set action relay
     next
     edit 2
          set sender ip-mask 23.103.144.0/22 <this is your MS365
     server IP address>
          set action relay
     next
     edit 3
          set sender-ip-mask 23.103.191.0/24 <this is your MS365
     server IP address>
          set action relay
     next
     edit 5
     ……
```

3. Add MS365 as a trusted relay on FortiMail.

Configuring Outbound Settings on Office 365

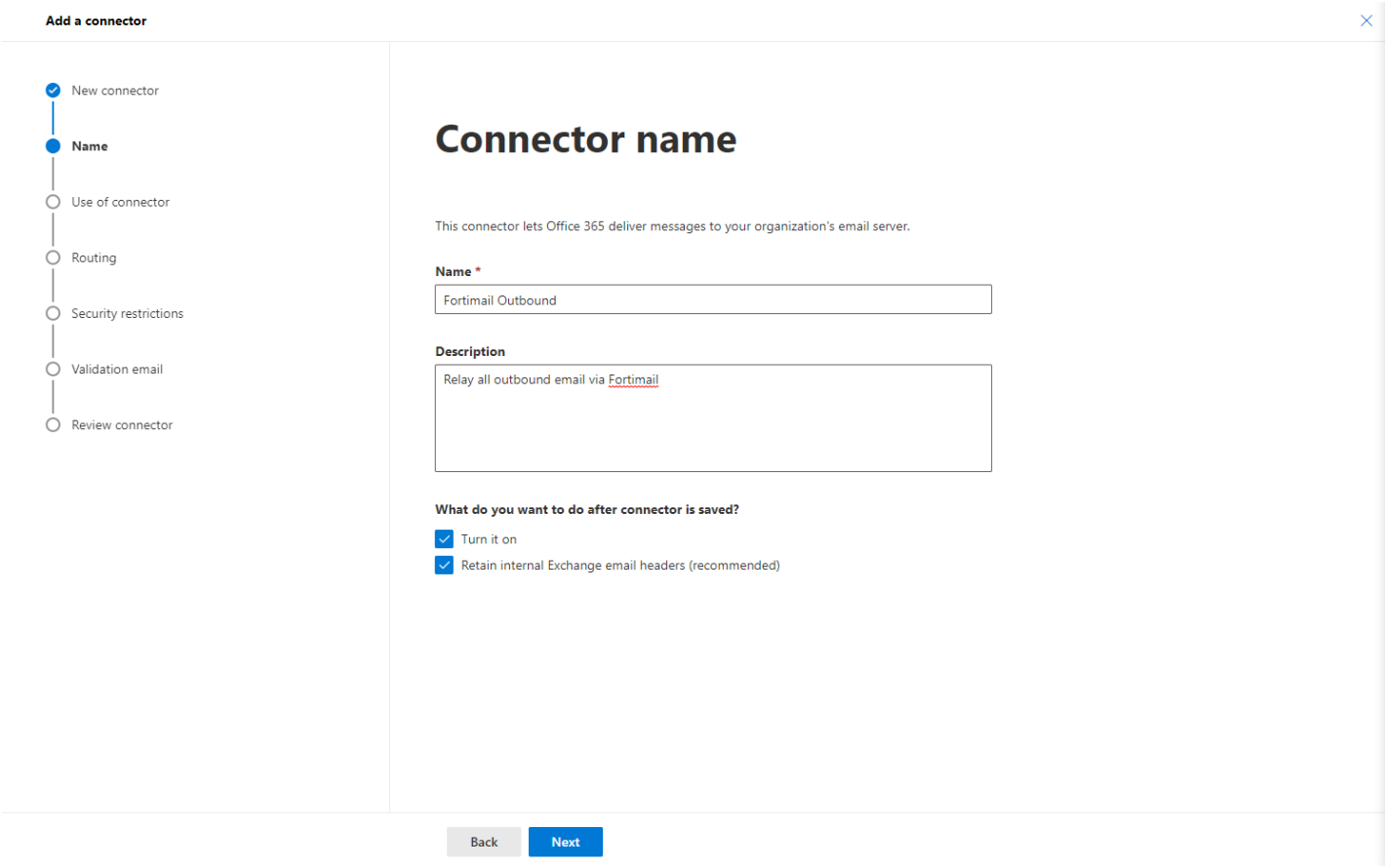
Now you need to configure MS365 to relay outgoing mail to FortiMail.

Configuring Outbound Connector on MS365

Outbound connectors are used to redirect outbound mail flow to a specific MTA instead of using the domain's configured MX records. Often this type of policy is created to meet a DLP and encryption requirement or to provide an additional level of antispam/malware inspection of outbound mail flow.

In this section you will create an outbound connector to deliver outbound email through FortiMail to provide that extra layer of email inspection.

1. Go to *Exchange Admin Center > Mail Flow > Connectors > Add a connector*.
2. Set *Connection from* to *Office 365* and set *Connection to* to *Partner organization*.
3. Select *Next*.
4. Enter a descriptive name and description.
5. Select *Next*.



6. Select the *Only when I have a transparent rule set up that redirects messages to this connector* radio button.

7. Select *Next*.
8. Configure the IP or FQDN of FortiMail Cloud.
   For example, if the hostname is example-com.fortimailcould.com, enter example-com.fortimailcould.com.
9. Select *Next*.
10. Select the *Any digital certificate, including self-signed certificates* radio button.
11. Select *Next*.
12. Select *Validate*. Office will now perform the steps necessary for validation. Enter username@<protected domain> and click *Validate*.
13. When the validation is finished, select *Close*. The *Status* section should display *Succeeded* if the process was successful.
14. Select *Save*.

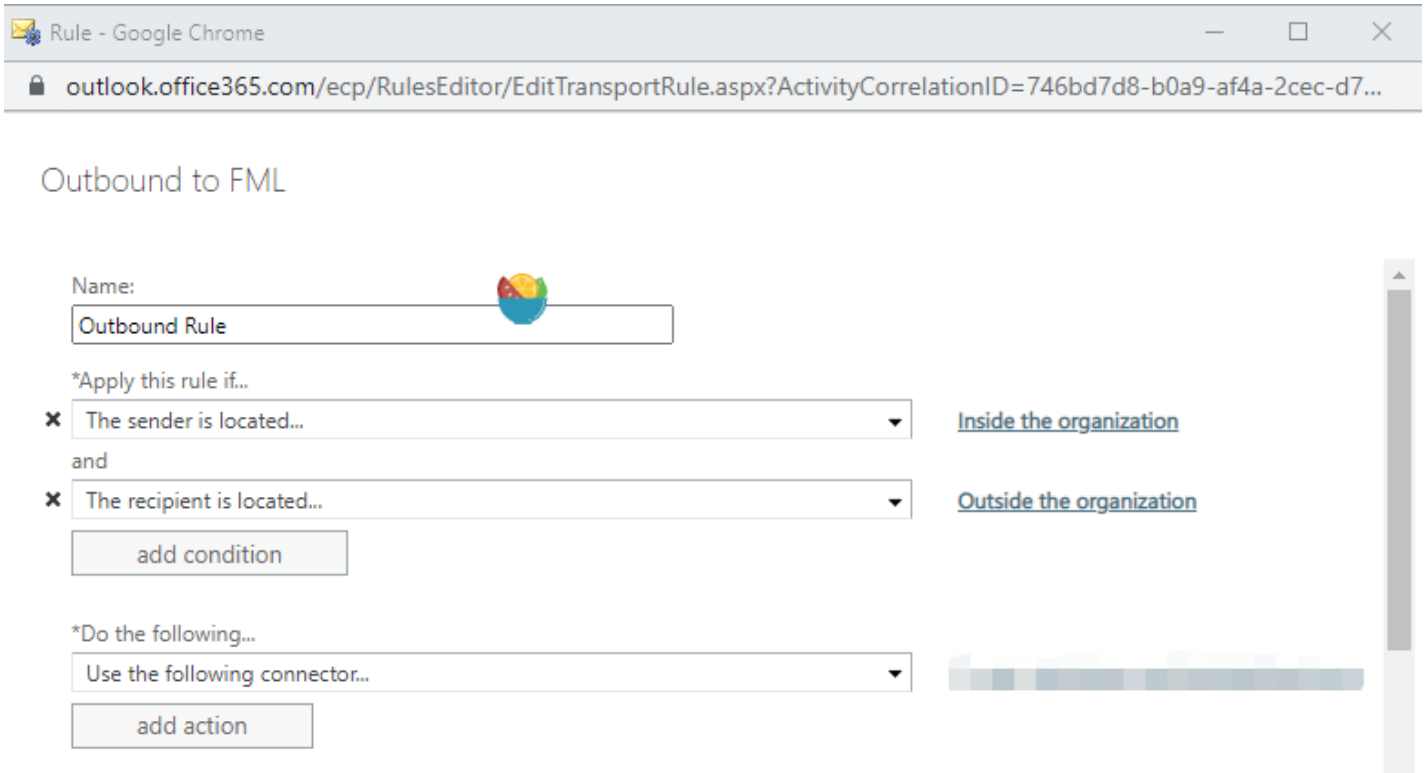
Configuring Outbound Transport Rule on MS365

Create a new transport rule to forward outbound messages through FortiMail for inspection using the connector defined above. The advantage of using a transport rule is that it is more granular in its application. With transport rules you can easily enable/disable the rules and require a combination of match conditions before the connector is utilized. On the other hand, the connector itself can only send all outbound messages.

TIP: Creating a test transport rule, that matches specific sender(s)/recipient(s) patterns, is a good method for testing an outbound connector without having to force all outbound traffic through it.

Note: Some match options are hidden by default. Click on the *More options* link to expand all additional match conditions.

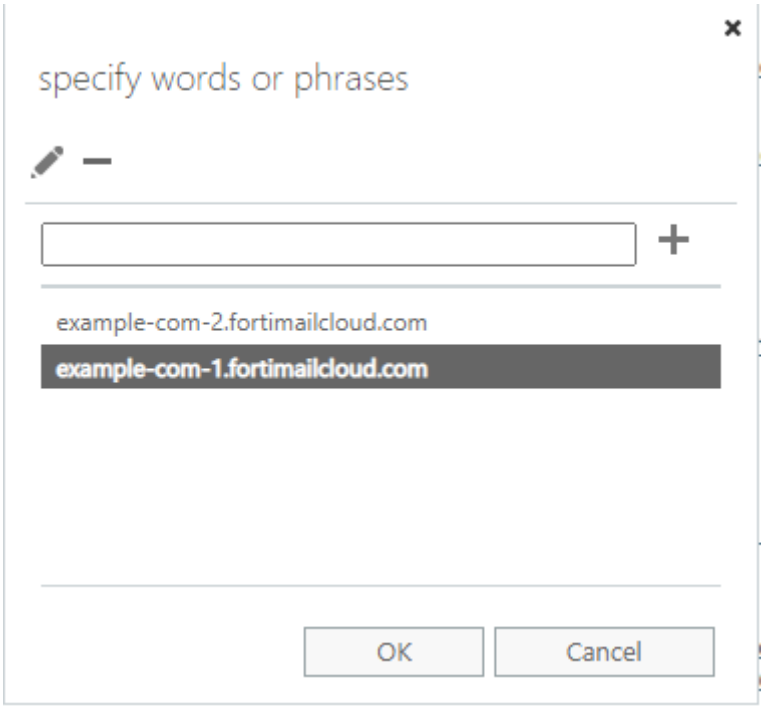
1. Log on to the Exchange admin center: https://admin.exchange.microsoft.com/#/homepage.
2. Select *Mail Flow*.
3. Select the plus sign (+) dropdown menu and select *Create a new rule…*
4. Click *More options* at the bottom.
5. Edit *Apply this rule if…*
6. Add condition under *Apply this rule if...*
7. Edit *Do the following* and enter the connector created in the previous step.



8. To avoid email loop, add an exception for your Fortimail Cloud instance by editing *Except if* > *A message header includes* > *Enter Received* as header name and entering below info as *specify words or phrases*.

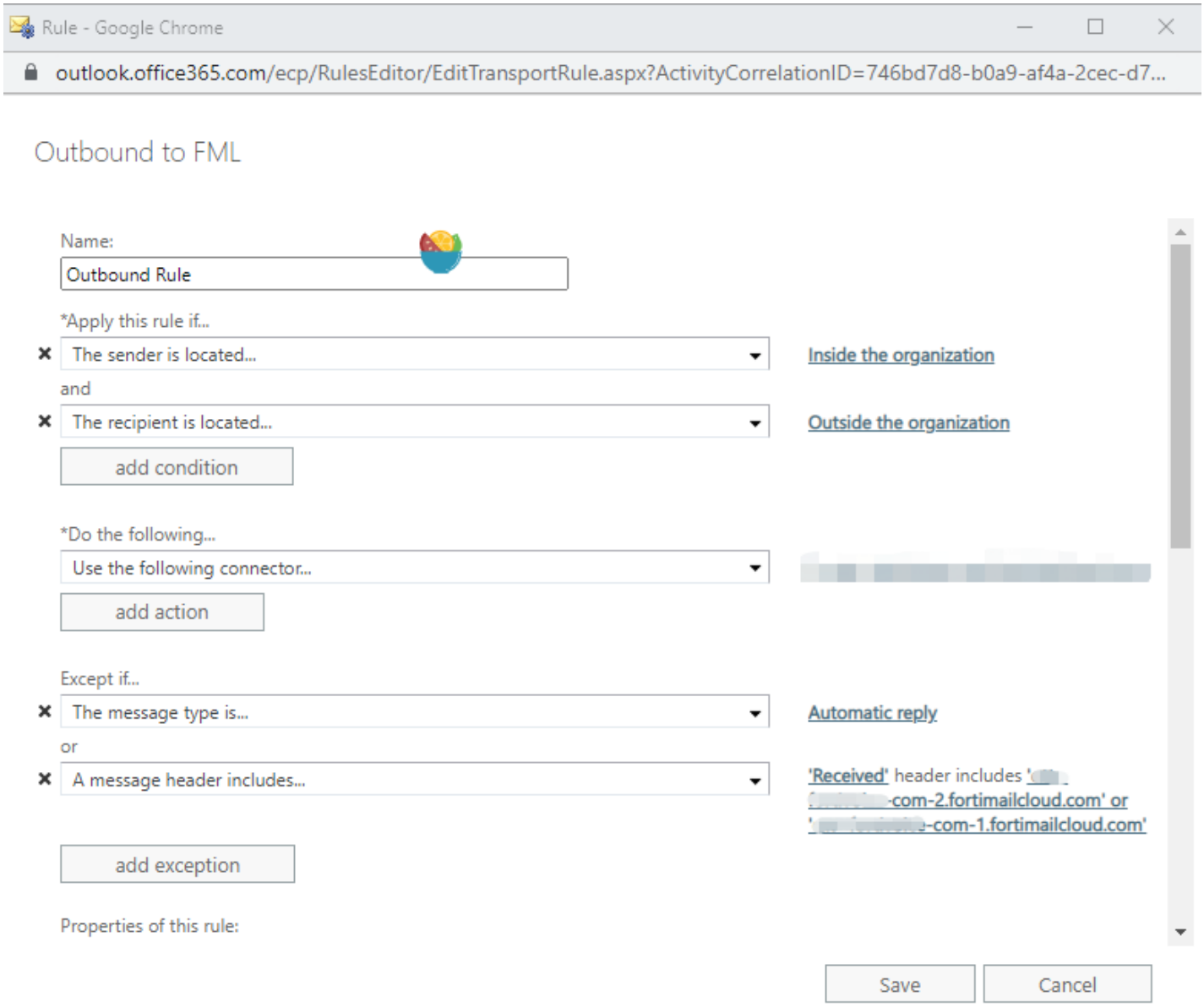
For example, if the hostname is example-com.fortimailcould.com, enter the following information:

```
example-com-1.fortimailcould.com
example-com-2.fortimailcould.com
```



This exception means that if the email has already been scanned by FortiMail Cloud, it will not be sent back again to FortiMail.

Then save the rule.



Your incoming and outgoing messages will now be protected by FortiMail Cloud. You should now apply a FortiMail antivirus and antispam profile.

Note: You can disable MS365 antispam services if you feel they are no longer required.



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.