FortiMail Cloud SMTP Recipient Verification with Microsoft 365 Deployment Guide

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

May 29, 2024

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-03-16	Initial release.
2024-05-29	Added “Enabling Exchange Online Protection”.

Introduction

This document outlines the steps to set up recipient verification in FortiMail Cloud with Microsoft Exchange.

The Microsoft Exchange mail server should reject email to non-existing users. If it's not configured properly, it may accept email to non-existing users. Regular mail servers should always have recipient filtering enabled to automatically reject emails to non-existing users. FortiMail Cloud utilizes recipient verification to count the number of mailboxes.

Prerequisite

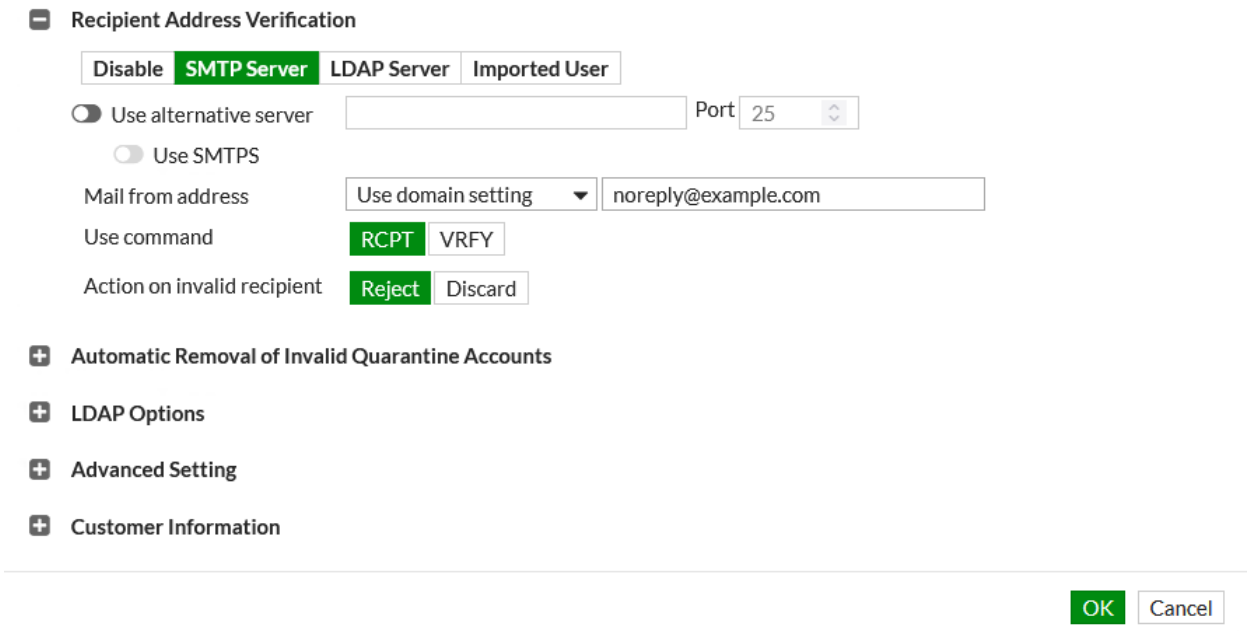
Follow this document to integrate FortiMail cloud with Microsoft 365 and make sure the email flow works properly.

For more information, see the FortiMail Cloud Integration with Microsoft 365 Deployment Guide in the Fortinet documentation library.

Configuring recipient address verification settings on FortiMail Cloud

You will first configure the FortiMail Cloud to change FortiMail's *Recipient address verification* from *Use system setting* to *Use domain setting*.

1. Go to the FortiMail Cloud user portal: https://www.fortimailcloud.com/main_page.
2. Select the FortiMail Cloud instance and login.
3. Select *Domain > Edit your protected domain example.com*.
4. Under *Recipient Address Verification*, select *SMTP Server.*
5. Set *Mail from address* to *Use domain setting* and enter your mail from address. (e.g. noreply@example.com)
6. Click *OK*.



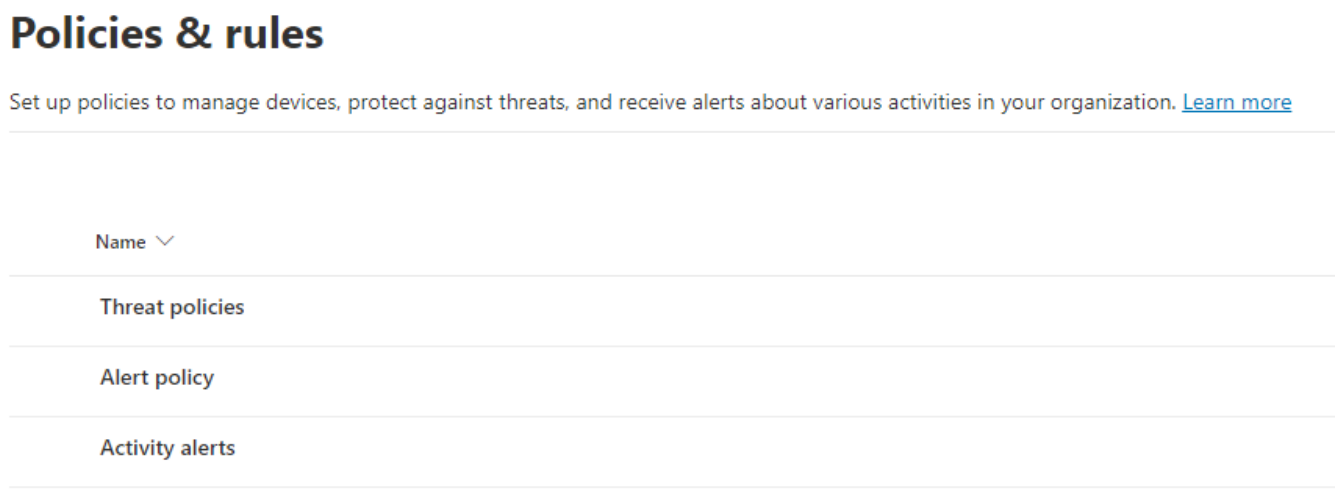
Configuring settings on Microsoft 365

Next you must configure Microsoft 365 to ensure recipient verification works properly.

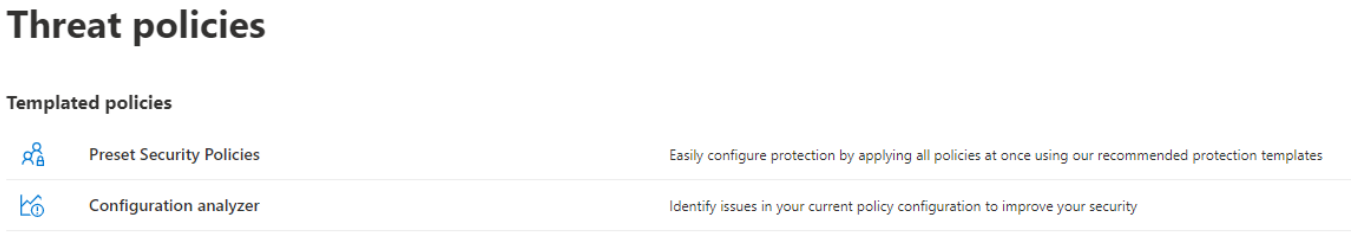
Enabling Exchange Online Protection

To enable Recipient Verification in Microsoft 365, the first step is to check if the Exchange Online Protection is enabled for your domain (or specific recipients). For some Microsoft 365 accounts, this feature is enabled by default.

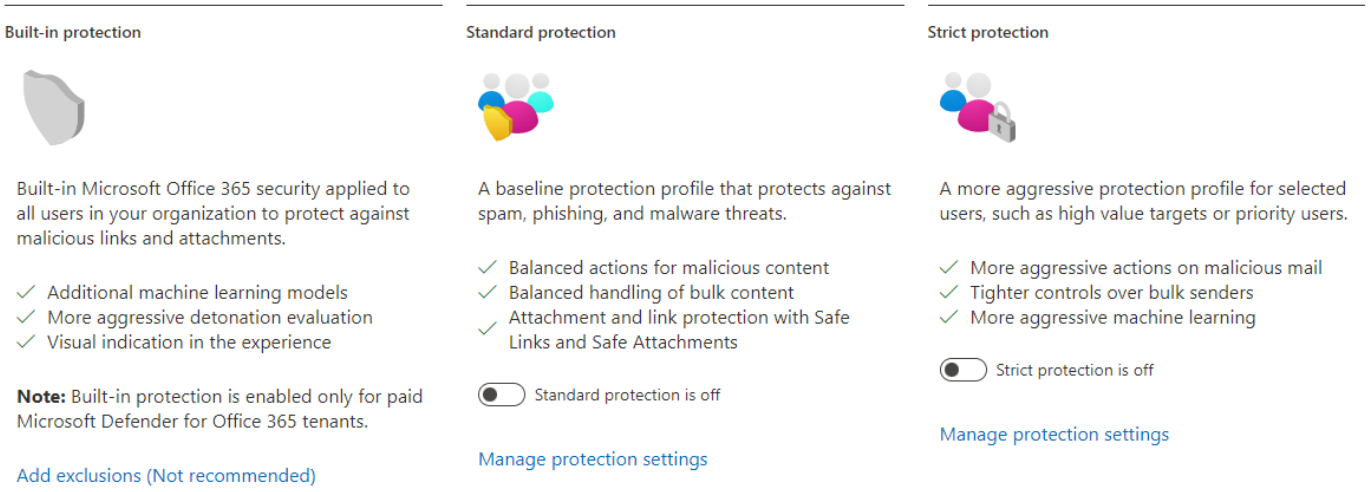
1. Go to *Microsoft Defender* > *Email & collaboration* > *Policies & rules.*



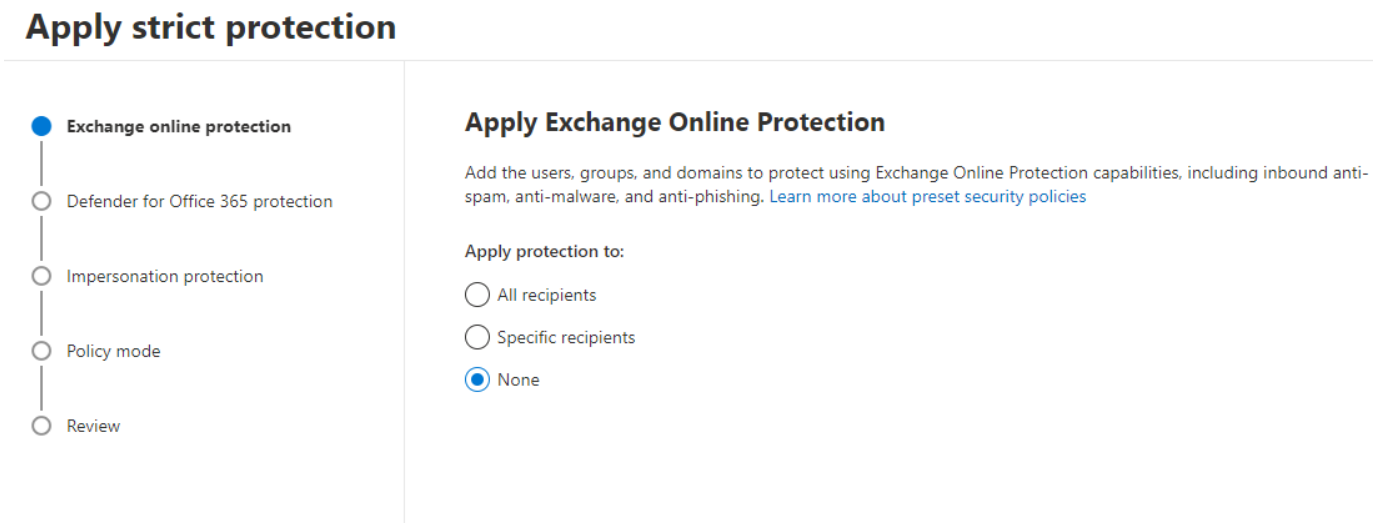
2. Select *Threat policies.*



3. Under *Templated policies*, select *Preset Security Policies.* There are three levels of protection available for a free Microsoft 365 tenant, and only Standard / Strict protection available for paid tenants, because the Built-in protection is enabled by default.



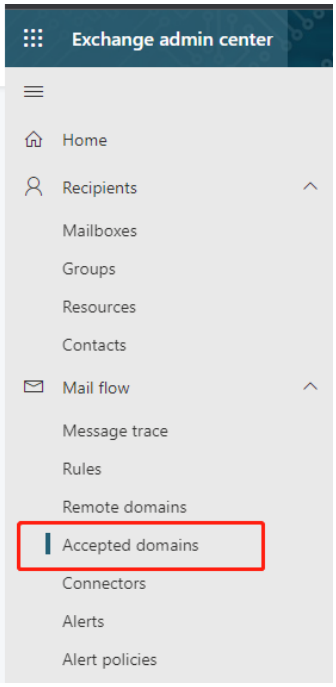
4. You can enable each level of the protection or customize the policies. Below is an example.



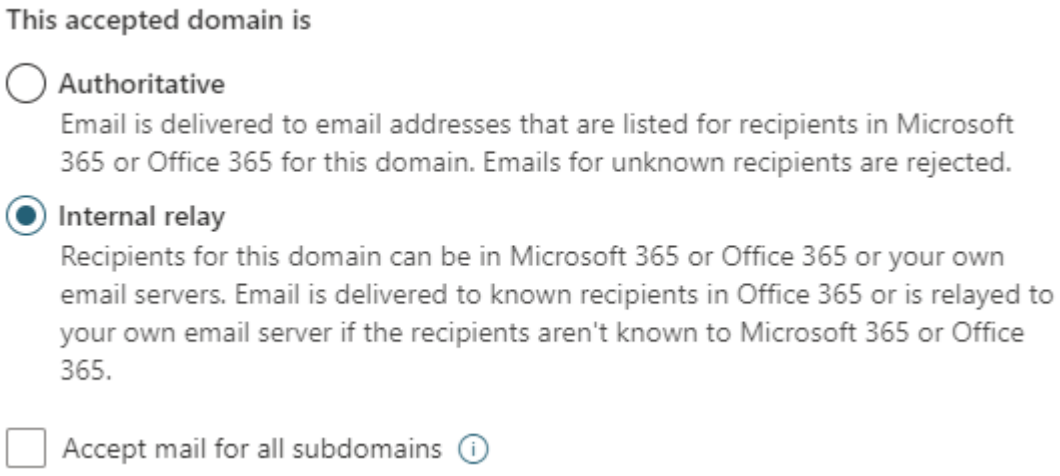
Configuring Directory Based Edge Blocking (DBEB)

You need to configure the accepted domains on Microsoft 365.

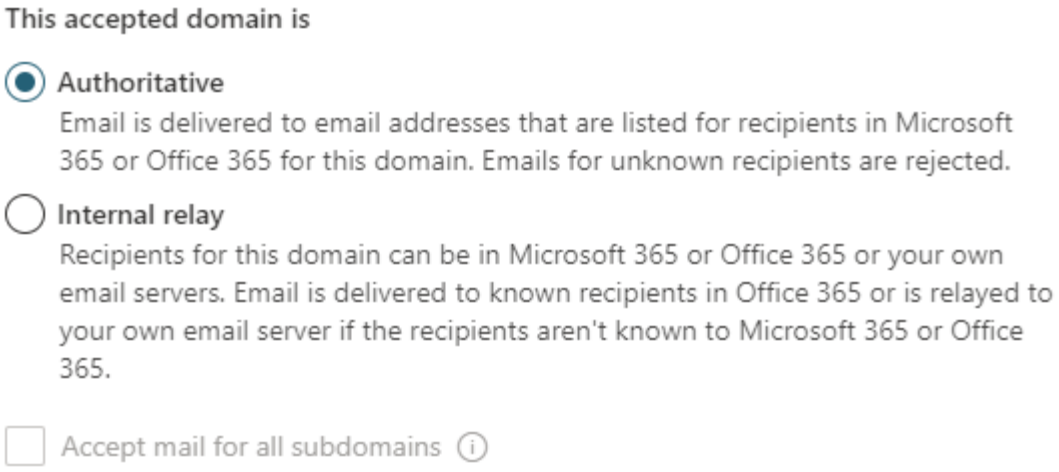
1. In Microsoft 365, go to *Exchange admin center* > *Mail flow* > *Accepted domains*.



2. Select your domain (example.com) and click *Edit*.
3. Ensure that the domain type is set to *Internal relay* and click *Save*. If it's set to *Authoritative*, change it back to *Internal relay* and click *Save*.
   Warning: You must complete this step and next step to make it work. Even if the original domain type setting is *Authoritative*, you have to change it back to *Internal relay* and then set it to *Authoritative*.



4. Then go back to go to *Exchange admin center > Mail flow > Accepted domains.* Select the domain and click *Edit*. Set the domain type to *Authoritative* and click *Save*.



Testing recipient verification

Perform the following processes to test the recipient verification with Microsoft 365

To test the recipient verification with Microsoft 365

1. Directly telnet to the Microsoft 365 server and verify the invalid mail user is rejected due to “Recipient address rejected”

```
telnet example-com0i.mail.protection.outlook.com 25
Trying 104.47.75.XXX...
Connected to example-com0i.mail.protection.outlook.com.
ehlo example.com
250-xxxxxx.mail.protection.outlook.com Hello [xxx.xxx.xxx.xxx]
250-SIZE 157286400
... ...
mail from:<noreply@example.com>
250 2.1.0 Sender OK
rcpt to:<thisisinvalidmailuser@example.com>
550 5.4.1 Recipient address rejected: Access denied.
```

If verification fails, please contact the Microsoft support team and work with them to make recipient verification work properly when directly connecting via telnet to the M365 server.

2. Directly telnet to the M365 server and verify you can receive “Recipient ok” for valid mail users

```
telnet example-com0i.mail.protection.outlook.com 25
Trying 104.47.75.XXX...
```

```
Connected to example-com0i.mail.protection.outlook.com.
ehlo example.com
250-xxxxxx.mail.protection.outlook.com Hello [xxx.xxx.xxx.xxx]
250-SIZE 157286400
... ...
mail from:<noreply@example.com>
250 2.1.0 Sender OK
rcpt to:<validmailuser@example.com>
250 2.1.5 <validmailuser@example.com>... Recipient ok
```

To test recipient verification with FortiMail Cloud

1. Telnet to your FortiMail Cloud server and verify it is rejected due to “Recipient address rejected”. Perform the test with both the primary and secondary FortiMail Cloud servers:

- example-com-1.fortimailcloud.com
- example-com-2.fortimailcloud.com

```
telnet example-com-1.fortimailcloud.com 25
220 xxx.fortimailcloud.com ESMTP ready
ehlo example.com
250-xxx.fortimailcloud.com
... ....
MAIL from:<noreply@example.com>
250 2.0.0 OK
RCPT to:<thisisinvalidmailuser@example.com>
550 5.4.1  Recipient address rejected: Access denied.


telnet example-com-2.fortimailcloud.com 25
220 xxx.fortimailcloud.com ESMTP ready
ehlo example.com
250-xxx.fortimailcloud.com
... ....
MAIL from:<noreply@example.com>
250 2.0.0 OK
RCPT to:<thisisinvalidmailuser@example.com>
550 5.4.1  Recipient address rejected: Access denied.
```

2. Telnet to your FortiMail Cloud server and verify that you can receive “Recipient ok” for valid mail users. Do the test with both primary and secondary FortiMail Cloud servers:

```
telnet example-com-1.fortimailcloud.com 25
```

```
220 xxx.fortimailcloud.com ESMTP ready
ehlo example.com
250-xxx.fortimailcloud.com
... ....
MAIL from:<noreply@example.com>
250 2.0.0 OK
RCPT to:<validmailuser@example.com>
250 2.1.5 <validmailuser@example.com>... Recipient ok

telnet example-com-2.fortimailcloud.com 25
220 xxx.fortimailcloud.com ESMTP ready
ehlo example.com
250-xxx.fortimailcloud.com
... ....
MAIL from:<noreply@example.com>
250 2.0.0 OK
RCPT to:<validmailuser@example.com>
250 2.1.5 <validmailuser@example.com>... Recipient ok
```