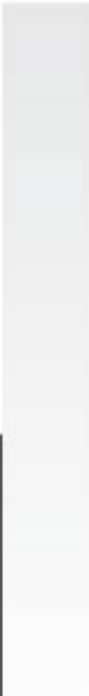


# FortiMail Cloud SMTP Recipient Verification with Microsoft 365 Deployment Guide



**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](mailto:techdocs@fortinet.com)



May 29, 2024

# TABLE OF CONTENTS

Change Log.....	4
Introduction .....	5
Prerequisite .....	5
Configuring recipient address verification settings on FortiMail Cloud .....	5
Configuring settings on Microsoft 365 .....	6
Enabling Exchange Online Protection .....	6
Configuring Directory Based Edge Blocking (DBEB) .....	7
Testing recipient verification .....	9
To test the recipient verification with Microsoft 365 .....	9
To test recipient verification with FortiMail Cloud.....	10

# 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](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](mailto:noreply@example.com))
6. Click *OK*.

**Recipient Address Verification**

Disable **SMTP Server** LDAP Server Imported User

Use alternative server  Port 25

Use SMTPS

Mail from address Use domain setting

Use command **RCPT** VRFY

Action on invalid recipient **Reject** Discard

**+ Automatic Removal of Invalid Quarantine Accounts**

**+ LDAP Options**

**+ Advanced Setting**

**+ Customer Information**

OK Cancel

# 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*.

### Policies & rules



Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. [Learn more](#)

Name ▾
Threat policies
Alert policy
Activity alerts

2. Select *Threat policies*.

### Threat policies

#### Templated policies

 Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
 Configuration analyzer	Identify issues in your current policy configuration to improve your security

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.

#### Built-in protection



Built-in Microsoft Office 365 security applied to all users in your organization to protect against malicious links and attachments.

- ✓ Additional machine learning models
- ✓ More aggressive detonation evaluation
- ✓ Visual indication in the experience

**Note:** Built-in protection is enabled only for paid Microsoft Defender for Office 365 tenants.

[Add exclusions \(Not recommended\)](#)

#### Standard protection



A baseline protection profile that protects against spam, phishing, and malware threats.

- ✓ Balanced actions for malicious content
- ✓ Balanced handling of bulk content
- ✓ Attachment and link protection with Safe Links and Safe Attachments

Standard protection is off

[Manage protection settings](#)

#### Strict protection



A more aggressive protection profile for selected users, such as high value targets or priority users.

- ✓ More aggressive actions on malicious mail
- ✓ Tighter controls over bulk senders
- ✓ More aggressive machine learning

Strict protection is off

[Manage protection settings](#)

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

### Apply strict protection

Exchange online protection

Defender for Office 365 protection

Impersonation protection

Policy mode

Review

#### Apply Exchange Online Protection

Add the users, groups, and domains to protect using Exchange Online Protection capabilities, including inbound anti-spam, anti-malware, and anti-phishing. [Learn more about preset security policies](#)

Apply protection to:

All recipients

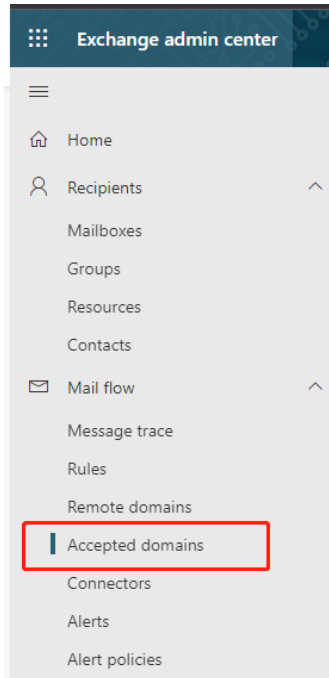
Specific recipients

None

## 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*.

This accepted domain is

- Authoritative**  
Email is delivered to email addresses that are listed for recipients in Microsoft 365 or Office 365 for this domain. Emails for unknown recipients are rejected.
- Internal relay**  
Recipients for this domain can be in Microsoft 365 or Office 365 or your own email servers. Email is delivered to known recipients in Office 365 or is relayed to your own email server if the recipients aren't known to Microsoft 365 or Office 365.
- Accept mail for all subdomains ⓘ

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*.

This accepted domain is



**Authoritative**

Email is delivered to email addresses that are listed for recipients in Microsoft 365 or Office 365 for this domain. Emails for unknown recipients are rejected.



**Internal relay**

Recipients for this domain can be in Microsoft 365 or Office 365 or your own email servers. Email is delivered to known recipients in Office 365 or is relayed to your own email server if the recipients aren't known to Microsoft 365 or Office 365.



Accept mail for all subdomains ⓘ

## 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.
```

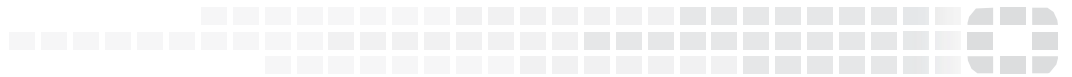
```
telnet example-com-2.fortimailcloud.com 25
220 xxx.fortimailcloud.com ESMTP ready
ehlo example.com
250-xxx.fortimailcloud.com
...
MAIL from:<noreply@example.com>
250 2.0.0 OK
RCPT to:<thisisinvalidmailuser@example.com>
550 5.4.1 Recipient address rejected: Access denied.
```

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
```



Copyright© 2024 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.