# Release Notes

**FortiMail 7.4.5**

**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO LIBRARY**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

August 29, 2025
FortiMail 7.4.5 Release Notes
06-745-1149368-20250829

# TABLE OF CONTENTS

# Change Log

The following is a list of documentation changes. For a list of software changes, see the other contents of this document.

| Date | Change Description |
|---|---|
| 2025-04-17 | Initial release of FortiMail 7.4.5 Release Notes. |

# Introduction and Supported Models

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 7.4.5 mature release, build 608.

For more FortiMail documentation, see the Fortinet Document Library.

## Supported models

| | |
|---|---|
| **FortiMail** | 200F, 400F, 900F, 2000E, 2000F, 3000E, 3200E, 3000F |
| **FortiMail VM** | • VMware vSphere Hypervisor ESX/ESXi 7.0, 8.0 and later<br>• Microsoft Hyper-V Server 2016, 2019, and 2022<br>• KVM qemu 2.12.1 and later<br>• Citrix XenServer v5.6sp2, 6.0 and later; Open Source XenServer 7.4 and later<br>• Alibaba Cloud BYOL<br>• AWS BYOL and On-Demand<br>• Azure BYOL and On-Demand<br>• Google Cloud Platform BYOL<br>• Oracle Cloud Infrastructure BYOL |

# Special Notices

This section highlights the special notices that should be taken into consideration before upgrading your platform.

## Communication between HA secondary units

Due to the introduction of primary backup in active-active HA in FortiMail 7.4.0, communication between the secondary units is also required. In config-only HA before FortiMail 7.4.0, it was not required.

## HA heartbeat and DHCP

If you upgrade from FortiMail 7.4.2 or earlier, and if the HA heartbeat's network interfaces have dynamic addresses such as DHCP, then you must either:

- before the upgrade, use static IP addresses instead
- after the upgrade:
  **a.** Immediately log in to all units in the cluster.
  **b.** Re-configure the heartbeat interfaces with their current IP addresses from the DHCP server.
  **c.** Reset the primary/secondary role if necessary, so that only one unit is the primary.

Cloud deployments (such as on Microsoft Azure) may commonly or by default use DHCP, requiring this setting change or procedure.

## TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiMail configurations and replace them with factory default settings.

## Monitor settings for the GUI

To view all objects in the GUI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280 x 1024.

# SSH connection

For security reasons, starting from FortiMail 5.4.2, FortiMail does not support SSH connections with plain-text password authentication. Instead, a challenge/response should be used.

# FortiGuard web filtering category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency web sites. In order to use the new categories, customers must upgrade their Fortinet products to one of the versions below.

- FortiMail 7.0.7, 7.2.5, 7.4.1 or later

# Product Integration and Support

## FortiNDR support

- Version 7.0.0

## FortiIsolator support

- FortiIsolator 2.3 and later

## FortiAnalyzer Cloud support

- Version 7.0.3

## AV Engine

- Version 6.00297

## Recommended browsers

**For desktop computers:**

- Google Chrome 135
- Mozilla Firefox 136
- Microsoft Edge 135
- Safari 17

**For mobile devices:**

- Official Google Chrome browser for Android 15
- Official Safari browser for iOS 18

Other browser versions have not been tested, but may fully function.

Other web browsers may function correctly, but are not supported by Fortinet.

# Firmware Upgrade and Downgrade

Before any firmware upgrade or downgrade, save a copy of your FortiMail configuration by going to *Dashboard* > *Status* and click *Backup* in the *System Information* widget.

After any firmware upgrade or downgrade, if you are using the web UI, clear the browser cache prior to login on the FortiMail unit to ensure proper display of the GUI screens. Also go to verify that the build number and version number match the image loaded.

The antivirus signatures included with an image upgrade may be older than those currently available from the Fortinet FortiGuard Distribution Network (FDN). Fortinet recommends performing an immediate antivirus signature update as soon as possible.

Firmware downgrading is not recommended and not supported in general. Before downgrading, consult Fortinet Technical Support first.

## Upgrade path

**6.0.5** (build 148) > **6.2.4** (build 272) > **6.4.5** (build 453) > **7.0.6** (build 216) > **7.2.2** (build 380) > **7.4.5** (build 608)

## Firmware downgrade

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- network interface IP address or management IP address
- static route table
- DNS settings
- administrator accounts
- administrator access profiles

# Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

## Antispam/Antivirus

| Bug ID | Description |
|---|---|
| 1133812 | In some cases, the DLP exception rule does not work properly. |
| 1143785 | Removed or modified file extensions are not detected by the content filter. |

## Mail Delivery

| Bug ID | Description |
|---|---|
| 1097318 | Email with disposition 'Accept;Defer Disposition' stays in the mail queue for a long time. |

## System

| Bug ID | Description |
|---|---|
| 1137553 | Gratuitous ARP from the IP pool is not sent during HA failover. |
| 1100041 | Failure to release or delete email using quarantine reports in Gmail. |
| 1144660 | MS365 API user list view search should be case insensitive. |
| 1142787 | Fail to open quarantined email if the folder name contains Japanese. |
| 1097114 | IBE users must log in twice to access the encrypted email. |

# Log and Report

| Bug ID | Description |
|---|---|
| 1122451 | IP addresses which users use when changing their credentials are not included in the relevant system event logs. |

# Common Vulnerabilities and Exposures

FortiMail 7.4.5 is no longer vulnerable to the following CVE/CWE-References.

Visit https://fortiguard.com/psirt for more information.

| Bug ID | Description |
|---|---|
| 985968 | CWE-613: Insufficient Session Expiration |
| 1147094 | CVE-2025-32756: Stack-based Buffer Overflow (CWE-121) |

www.fortinet.com