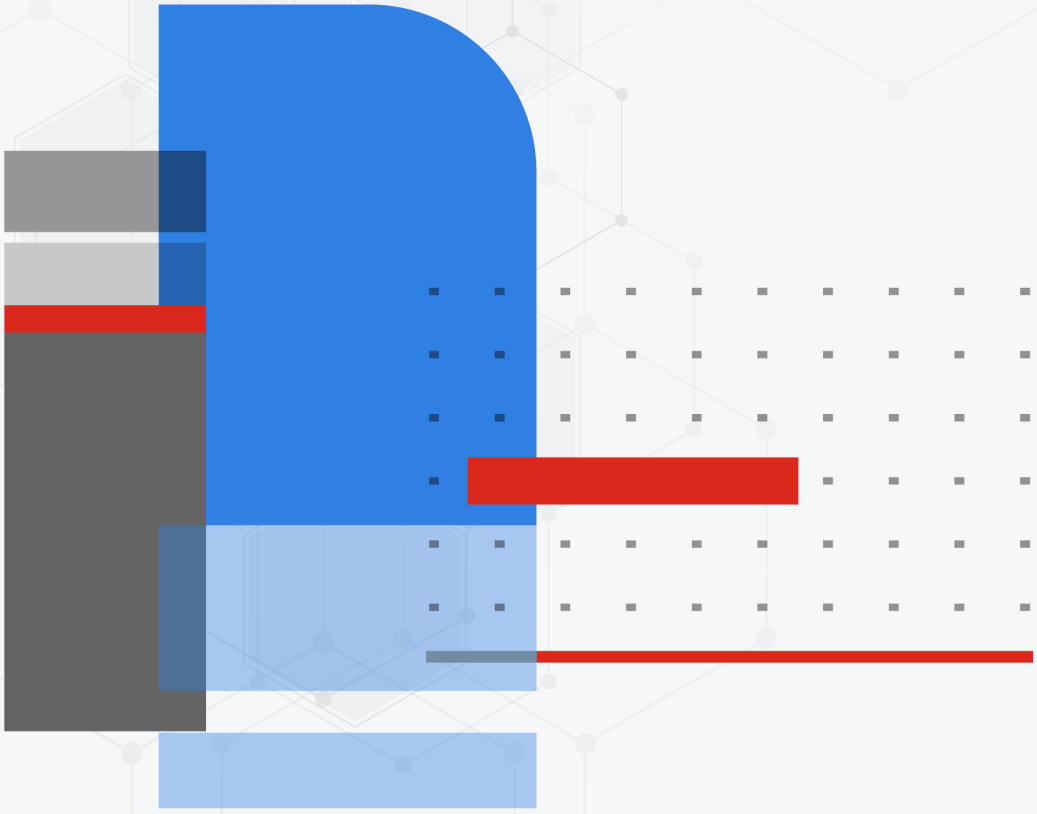
Release Notes

FortiMail 7.2.8



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

April 17, 2025
FortiMail 7.2.8 Release Notes
06-727-1149366-20250417

TABLE OF CONTENTS

Change Log **4**
Introduction and Supported Models **5**
Supported models 5
Special Notices **6**
TFTP firmware install 6
Monitor settings for the web UI 6
SSH connection 6
FortiGuard web filtering category v10 update 6
Product Integration and Support **7**
FortiNDR support 7
FortiIsolator support 7
FortiAnalyzer Cloud support 7
AV Engine 7
Recommended browsers 7
Firmware Upgrade and Downgrade **8**
Upgrade path 8
Firmware downgrade 8
Resolved Issues **9**
Antispam/Antivirus 9
Mail Delivery 9
System 9
Log and Report 9
Common Vulnerabilities and Exposures 10

Change Log

Date	Change Description
2025-04-17	Initial release.

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 7.2.8 release, build 423.

For 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 higher • Microsoft Hyper-V Server 2016, 2019, 2022 • KVM qemu 2.12.1 and higher • Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher • AWS BYOL and On-Demand • Azure BYOL • Google Cloud Platform BYOL • Oracle Cloud Infrastructure BYOL

Special Notices

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

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 web UI

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

SSH connection

For security reasons, starting from 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, 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 - Fixed in 7.0.7, 7.2.5, 7.4.1.

Product Integration and Support

FortiNDR support

- Version 7.0.0

FortiIsolator support

- FortiIsolator 2.3 and above

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 web UI 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 AV 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) > **7.2.8** (build 423)

Firmware downgrade

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

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user accounts
- admin 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
1111258	Match all condition "Body is Empty" and "Empty subject regex" in the DLP profile is not triggered.

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.
1089762	Scheduled reports are delivered later than expected.
1107735	Failure to release system quarantined email.
1100041	Failure to release or delete email using quarantine reports in Gmail.

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 7.2.8 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