

Release Notes

FortiMail 7.2.9



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

December 04, 2025

FortiMail 7.2.9 Release Notes

06-729-1232797-20251204

TABLE OF CONTENTS

Change Log	4
Introduction and Supported Models	5
Supported models	5
What's New	6
What's Changed	7
Special Notices	8
TFTP firmware install	8
Monitor settings for the web UI	8
SSH connection	8
FortiGuard web filtering category v10 update	8
Product Integration and Support	9
FortiNDR support	9
Fortisolator support	9
FortiAnalyzer Cloud support	9
Recommended browsers	9
Firmware Upgrade and Downgrade	10
Upgrade path	10
Firmware downgrade	10
Resolved Issues	11
System	11
Common Vulnerabilities and Exposures	11
Known Issues	12

Change Log

Date	Change Description
2025-12-04	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 7.2.9 release, build 430.

For FortiMail documentation, see the [Fortinet Document Library](#).

Supported models

FortiMail	200F, 400F, 900F, 2000E, 2000F, 3000E, 3200E, 3000F
FortiMail VM	<ul style="list-style-type: none">• 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• Azure BYOL• Google Cloud Platform BYOL• Oracle Cloud Infrastructure BYOL

What's New

No new features have been added to this patch release.

What's Changed

No changes have been made to this patch release.

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

Fortisolator support

- Fortisolator 2.3 and above

FortiAnalyzer Cloud support

- Version 7.0.3

Recommended browsers

For desktop computers:

- Google Chrome 142
- Mozilla Firefox 145
- Microsoft Edge 142
- Safari 26

For mobile devices:

- Official Google Chrome browser for Android 16
- Official Safari browser for iOS 26

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) > **7.2.9** (build 430)

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 inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

System

Bug ID	Description
1161849	The system may crash intermittently with the error message: Failed to boot default entries.
1156491	DKIM keys may get lost in the configuration.

Common Vulnerabilities and Exposures

FortiMail 7.2.9 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1174554	CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')
1189174	CWE-358: Improperly Implemented Security Check for Standard

Known Issues

No known issues have been found in this patch release.

