



Release Notes

FortiMail 7.4.9



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

October 05, 2026

FortiMail 7.4.9 Release Notes

TABLE OF CONTENTS

Change Log	4
Introduction and Supported Models	5
Supported models	5
What's New and What's Changed	6
Special Notices	7
HA considerations	7
Product Integration and Support	8
FortiGuard Antivirus Engine:	8
FortiNDRsupport	8
FortiAnalyzer Cloud support	8
Recommended browsers	8
Firmware Upgrade and Downgrade	9
Upgrade path	9
Firmware downgrade	9
Resolved Issues	10
System	10
Administrator GUI/Webmail	10
Common Vulnerabilities and Exposures	10

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
2026-10-03	Initial release of FortiMail 7.4.9 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 7.4.9 mature release, build 630.

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 Microsoft Hyper-V Server 2016, 2019, 2022, and 2025 KVM qemu 2.12.1 and later Citrix XenServer v5.6sp2, 6.0 and later; Open Source XenServer 7.4 and later Alibaba Cloud BYOL Amazon AWS BYOL Microsoft Azure BYOL Google Cloud Platform BYOL Oracle Cloud Infrastructure BYOL

What's New and What's Changed

The following table summarizes the new features, enhancements, and changes in this release. For details, see the [FortiMail Administration Guide](#) and [FortiMail CLI Reference](#).

Feature	Description
Permanent DST for Alberta and Manitoba, Canada	After British Columbia, these two Canadian provinces decided to adopt permanent year-round DST in 2026. This release includes the new DST changes. If your FortiMail system is located in these Canadian provinces, you can select the new time zone to accord with the clock changes.

Special Notices

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

HA considerations

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 v7.4.2 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.

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

Product Integration and Support

FortiGuard Antivirus Engine:

- Version 6.00297

FortiNDR support

- Version 7.0.0

FortiAnalyzer Cloud support

- Version 7.0.3

Recommended browsers

For computers:

- Google Chrome 154
- Microsoft Edge 153
- Mozilla Firefox 157
- Apple Safari 27

For mobile devices:

- Google Chrome browser for Android 17
- Safari browser for iOS 27

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) > **7.4.9** (build 630)

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

System

Bug ID	Description
1325385	IMAP disconnection issue.
1321218	In FIPS mode, DKIM is not displayed on the admin GUI and no DKIM signatures are added to outgoing email; and lower version OpenSSL fails to connect to FortiMail with an "EMS not enabled" error message.

Administrator GUI/Webmail

Bug ID	Description
1256400	Unknown server error "Internal error" when activating or launching the FortiCloud portal from the Dashboard.

Common Vulnerabilities and Exposures

FortiMail 7.4.9 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1303920	CWE- 22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
1303439	
1348679	
1335851	
1336260	
1335852	

Bug ID	Description
1318177	CWE- 1050: Excessive Platform Resource Consumption within a Loop

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.