Release Notes

FortiMail 7.6.4

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 07, 2025
FortiMail 7.6.4 Release Notes
06-764-1208562-20251007

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
2025-10-06	Initial release of the FortiMail 7.6.4 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 7.6.4 mature release, build 818.

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, and 2022 • 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 • AWS BYOL and On-Demand • Azure BYOL and On-Demand • Google Cloud Platform BYOL • Oracle Cloud Infrastructure BYOL

What's new

The following table summarizes the new features and enhancements in this release. For details, see the FortiMail Administration Guide and FortiMail CLI Reference.

Feature	Description

Queue runner enhancement (CLI only)	Added the following CLI command to allow smtpqd to run dynamically and more efficiently.
	`config system mailserver`
	`  set smtp-delivery-queue-runner-option enhanced`
	`end`

Option to use Envelope From or Header From as sender for recipient policy matches	Added the following CLI command to turn on the option on the admin GUI to use Envelope From or Header From as the sender when configuring recipient policies. Only Envelope From was used before.
	Note that this feature is only available with the Advanced Management license.
	`config system advanced-management`
	`  set recipient-policy-sender-option {envelope-from-only |`
	`  envelope-or-header-from }`
	`end`
	Default setting is `envelope-from-only`.

SSO supports multiple service providers	SSO supports two separate service provider (SP) entities for admin and webmail users.

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.

Firmware upgrade and downgrade

Before you upgrade or downgrade, back up your configuration and any other stored data. For details, see the FortiMail Administration Guide.

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 verify that the build number and version number match the image loaded, which indicates that the upgrade was successful.

The FortiGuard 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) > **7.4.3** (build 600) > **7.6.4** (build 818)

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

Firmware image checksums

When you download software, use checksums to verify that the file has not been modified or corrupted.

1. On the Fortinet Support site, go to *Downloads* > *Firmware Images*.
2. Select FortiMail
3. Click the *Download* tab and then click to go into the version folder.
4. Next to the file, click *HTTPS* to download the file. Then click *Checksum* to show the file's checksum.

   To verify the file's integrity, the checksum shown by the website should match the checksum of the file on your computer.
5. Use a checksum tool and compute the firmware file's checksum. For example, you could use certutil on the Windows command line:

   ```
   certutil -hashfile firmware.out SHA512
   ```

   If the file's checksum shown on the Fortinet Support website matches the file's checksum on your computer, then the file is intact.

Product integration and support

FortiNDR integration

- FortiNDR 7.0.0

FortiIsolator integration

- FortiIsolator 2.3 and later

FortiAnalyzer Cloud integration

- FortiAnalyzer Cloud 7.0.3

FortiGuard Antivirus Engine

- Version 7.00041

Recommended browsers

The FortiMail GUI has been tested on the following web browsers:

For computers:

- Apple Safari 18
- Google Chrome 140
- Microsoft Edge 140
- Mozilla Firefox 143

For mobile devices:

- Official Google Chrome browser for Android 16
- 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.

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
1165264	Embedded URLs in PDF attachments are not detected.
1172602	Files with .emf extension are incorrectly detected as application/zip files.
1163240	Email with image attachment is blocked by the content profile as password-protected file.
1184804	Wrong MIME type detection.
1183090	JPEG files are incorrectly detected as RAR files.
1200245	When sender address rate control reaches the limit and some email are in the FortiSandbox queue , FortiMail receives NoResult from FortiSandbox.
1199314	Invisible malicious URLs may not be detected.
1191454	Replacement message action in the content profile action does not work properly.
1194912	SPF check fails due to unknown modifiers.
1189764	Decompressed files with big size are not scanned or sent to quarantine.

Email delivery

Bug ID	Description
1180692	Fail to open encrypted email notification link after going through a third party security inspection.
1191404	Need to add missing HEADER FROM value.
110142	In some cases, email is modified even though Deliver to original host is set as Unmodified copy.

System

Bug ID	Description
1160450	When generating a certificate signing request (CSR), FortiMail does not add the X509v3 Subject Alternative Name (SAN) extension to the request.
1164834	After upgrading to v7.6.3 release, the HA pair is out of synchronization.
1163747	High CPU usage caused by mailfilterd.
1181505	High CPU usage without known reasons.
1209753	High CPU usage caused by DLP profiles.
1186768	IP address with port indication is not supported in email archiving destination.
1173175	Legitimate email caught by Intelligent Analysis.
1182035	In some cases, a block list entry may be missing in HA mode.
1195444	For FIPS-CC purpose, LDAPS needs to drop the non-approved and non certified algorithms / TLS versions.
1198879	Disabling use of non-FIPS approved algorithms in IBE, S/MIME, and SNMPv3.
1181436	Some disclaimer variables may not work properly.
1161849	After upgrading v7.4.3 to v7.6.3, the system began crashing intermittently with the error message: Failed to boot default entries.
1197184	Changing prohibited terms or dictionary profilesmay cause system freeze.
1189587	UNSEEN error returned from FortiSandbox.

Logs and reports

Bug ID	Description
1168320	Database error executing message in antispam logs.
1157617	In some cases, the miglogd process may run into a dead loop.

Administrator GUI/webmail

Bug ID	Description
1198315	Older JQuery-UI version is used.
1176950	Under Security > URL Filter > Profile, the total ref number does not display correctly.
1196837	In ForitMail webmail, encrypted email for Zoom session links is replaced with .ICS file attachment.
1194351	Character T and Z appear in FortiMail clawback timestamp for Quarantine Summary email template.
1195458	A report with a comma "," in its name cannot be generated or deleted.

Common Vulnerabilities and Exposures

FortiMail 7.6.4 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1189174	CWE-358: Improperly Implemented Security Check for Standard
1174554	CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')
1173145	CWE-312: Cleartext Storage of Sensitive Information
1173144	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere
1169607	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

www.fortinet.com

Copyright© 2025 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.