Release Notes

FortiMail 7.6.5

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

May 12, 2026
FortiMail 7.6.5 Release Notes
06-765-1288937-20260512

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
2026-05-12	Initial release of the FortiMail 7.6.5 Release Notes.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 7.6.5 mature release, build 831.

For more FortiMail documentation, see the Fortinet Document Library.

Supported models

FortiMail	200F, 400F, 900F, 900G, 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
SNMPv3 Support	Support for authentication protocol SHA256, SHA384, and SHA512, and encryption algorithm AES256.

What's changed

No behavior or configuration changes.

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) > **7.6.5** (build 831)

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 7.00051

Recommended browsers

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

For computers:

- Apple Safari 26
- Google Chrome 148
- Microsoft Edge 148
- Mozilla Firefox 150

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.

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
1280682	Password-protected XLS spreadsheet files were not be decrypted.
1277001	XLSX files inside of a `winmail.dat` file were incorrectly detected as XLS files.
1212055	Split QR codes in PDF files were not detected.
1215411	When the FortiSandbox timeout was reached, URL click protection returned an error message instead of allowing the URL according to the FortiSandbox timeout setting.
1236369	Color-coded URLs changed the URL format or category.
1237789	DMARC failure occurred for some valid senders.
1240303	Threat feed for a resource URL did not work properly.
1240477	URI redirect lookup did not work properly.
1244117	Content action in policy matches should have been classified as `Not spam` instead of `Spam`.
1213884	When the concurrent sessions were high, URI click protection did not work properly.
1267062	CDR did not work properly with some Microsoft Word files.
1226744	PDF QR code check should not have extracted embedded files.
1217442	After upgrading from v7.6.3 to v7.6.4, personal quarantine email cannot be released if the re-scan option is enabled.
1283521	Newsletter is not detected if FortiMail performs 'Expanding alias' based on the LDAP profile query.
1253268	Multi-line URL with hyphens is not handled properly.
1132000	Microsoft Office documents are detected as executable/vba although they do not contain any VBA scripts.

Email delivery

Bug ID	Description
1213935	If there were multiple long recipient addresses, then the `X-FEAS-BEC-Info:` message header was longer than 998 characters and not folded, which violates RFC 5322 section 2.1.1.
1212099	When there were multiple recipients and multiple matching policies, some recipients may not have received the email.
1237301	Email was dropped when there was an issue with the NAS server.
1239157	In some cases, email could not be sent. The error message was: `timeout before data read, where=eom`
1255101	Email delivery failed due to a DNS TXT record limit.
1255737	In some cases, email continuity did not work properly.
1286724	ZIP files containing BAT files were not detected by the content filter.

System

Bug ID	Description
1054198	On a primary unit in an HA group, quarantine search has intermittent issues.
1277031	Quarantine search took an abnormally long time.
1274586	Unable to remove DKIM selectors with underscores.
1256422	The most recently installed CA certificate was not effective in the CA chain.
1272888	In active-active HA mode, personal block/safe lists created during HA down time were not synchronized after HA was restored.
1217869	An OFTP connection with FortiAnalyzer 7.4.8 requires the correct certificate option.
1217884	STARTTLS was not initiated for authentication in relay host tests under *System* > *Mail Setting* . *Relay Host List*.
1254934	After an upgrade from FortiMail 7.6.4 to 7.6.5 interim release, the HA group was out of sync.
1235809 1223903	High CPU usage was caused by the PDF scan.
1249685	High CPU usage was caused by text extraction from images in the PDF scan.
1227816	After an upgrade from FortiMail 7.6.3 to 7.6.4, after the command `chattr sync-disable`, active-passive HA synchronization had issues.

Bug ID	Description
1222230	High CPU usage occurred on FML-900F models.
1220666	High CPU usage was caused by large files in the PDF scan.
1228791	High CPU usage was caused by regular expressions in the DLP scan.
1282440	Address map rewriting did not comply with RFC 2047 encoding for Cyrillic display names.
1290973	TLS signature algorithm still accepts SHA224 /DSA family.
1208387	When using FortiGate v7.6.3 with FortiMail v7.6.3, the security fabric cannot be established.
1167729	Fail to mount an external USB key.

Log and report

Bug ID	Description
1248953	After an uprade to FortiMail 7.6.4, regular expression errors were logged on every SSH login.
1232787	File names were not displayed correctly in logs.
1260702	Tables were truncated in downloaded PDF reports.
1284629	When there are multiple image attachments and one image is detected by 'Image Spam', there are no details in the log about which image was detected.

Administrator GUI/webmail

Bug ID	Description
1189608	In some cases, personal quarantine search did not work properly.
1272998	When logging into the administrative GUI using SSO, the administrator access profile that was applied (`admin_sso`) was not the profile that had been selected.
1265152	Quarantine email viewing issue with Mozilla Firefox.

Common Vulnerabilities and Exposures

FortiMail 7.6.5 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1241154	CWE-358: Improperly Implemented Security Check for Standard
1233871	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
1241590	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
1272856 1274518	CWE-476: NULL Pointer Dereference
1274537	CWE-358: Improperly Implemented Security Check for Standard
1234002	CWE-121: Stack-based Buffer Overflow
1286744	CWE-472: External Control of Assumed-Immutable Web Parameter

Known issues

No known issues.

www.fortinet.com