Release Notes

FortiMail 7.6.7





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 26, 2026
FortiMail 7.6.7 Release Notes

TABLE OF CONTENTS

4
Change log 5
Introduction and supported models 6
Supported models 6
Special notices 7
HA considerations 7
What's new 8
What's changed 9
Resolved issues 10
Antispam/antivirus 10
Email delivery 10
System 10
Log and report 11
Administrator GUI/webmail 11
Common Vulnerabilities and Exposures 11
Known issues 13
Firmware upgrade / downgrade path 14
Upgrade path 14
Firmware downgrade 14
Firmware image checksums 14
Product integration and support 16
FortiNDR integration 16
FortiAnalyzer Cloud integration 16
FortiGuard Antivirus engine 16
Recommended browsers 16

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
2026-10-02	Initial release of the FortiMail 7.6.7 Release Notes.
2026-10-26	Added auth password length limit change to What's Changed.

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 7.6.7 mature release, build 858.

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

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.

What's new

None.

What's changed

The following table summarizes the behavior and configuration changes in this release. For details, see the FortiMail Administration Guide and FortiMail CLI Reference.

Feature	Description
Permanent DST for British Columbia, Alberta, and Manitoba, Canada	These three 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 the three Canadian provinces, you can select the new time zone to accord with the clock changes.
Auth password length limit	Reduced from 139 to 96 characters.

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.

Antispam/antivirus

Bug ID	Description
1265528	QR code with a phishing URL was not blocked.
1302731	System blocklist does not work properly for some mails.
1337342	Dictionary scores in content profiles are not calculated correctly for attachment files.
1333263	Sender reputation score increases with Delivery action triggered.

Email delivery

Bug ID	Description
1309755	Mailfilter timeout errors.
1308700	Email delivery fails when MTA-STS is enabled in Monitor mode.
1351218	Delivery issue caused by long domain names.

System

Bug ID	Description
1309261	Incorrect time zone for Vilnius.
1303229	FIPS-CC mode does not work in HA.
1310340	SMTP client certificate selection issue with IP pools.
1296584	High CPU usage caused by file decryption in Microsoft & Google API mode.

Bug ID	Description
1321218	After upgrading to FortiMail 8.0.0 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.
1325385	IMAP TLS errors after upgrading to FortiMail 8.0.0.

Log and report

Bug ID	Description
1329850	"Sender Recipient Relationship license is expired" log message is misleading because the FortiMail system does not even have the license.

Administrator GUI/webmail

Bug ID	Description
1312746	Contact and Calendar pages in Webmail are not accessible when logging in with SSO.
1304284	Customized webmail login template fails to display authentication error message for incorrect credentials.
1323501	Cyrillic character display issue.
1298828	Webmail sent folder email display issue after mail migration.
1265152	Quarantine email viewing issue with Mozilla Firefox.

Common Vulnerabilities and Exposures

FortiMail 7.6.7 is no longer vulnerable to the following CVE/CWE-References.

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

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

Bug ID	Description
1335851 1336260 1335852	
1303443	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
1318177	CWE-1050: Excessive Platform Resource Consumption within a Loop
1286744	CWE-472: External Control of Assumed-Immutable Web Parameter

Known issues

None.

Firmware upgrade / downgrade path

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 832) > **7.6.7** (build 858)

Firmware downgrade

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

- operation mode
- interface IP address/management IP address
- static route table
- DNS settings
- administrator accounts
- administrator 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

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:

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

For mobile devices:

- Official Google Chrome browser for Android 17
- Official 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.

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.