Release Notes

FortiMail 8.0.2





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 8.0.2 Release Notes

TABLE OF CONTENTS

Change log **4**
Introduction and supported models **5**
Supported models 5
Special notices **6**
HA considerations 6
What's new **7**
Antispam/antivirus/content 7
Email delivery 7
System 7
GUI 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 12
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
2026-10-03	Initial release of the FortiMail 8.0.2 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 8.0.2 feature release, build 263.

For more FortiMail documentation, see the Fortinet Document Library.

Supported models

FortiMail	200F, 400F, 900F, 900G, 2000F, 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

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

Antispam/antivirus/content

Feature	Description
OCR scan (license required)	In *System* > *FortiGuard* > *Licensed Feature*, if you have the license for Optical Character Recognition (OCR), you can now enable that service. When a content profile is used for an image analysis scan, OCR can recognize text in images that are in the email body, PDF, and Word attachments. The recognized text can be reused by other URL-based and text-based scans. For details, see how to use OCR.

Email delivery

Feature	Description
Support mail routing in ACL delivery rules	In *Policy* > *Access Control* > *Delivery*, you can now specify *Relay host* for mail routing. This can be useful to route mail for some senders or recipients to a different SMTP gateway or mail host, especially if you have already defined those groups in an LDAP directory query.

System

Feature	Description
DNS cache TTL maximum	In `config system dns`, you can now specify `cache-max-ttl`. Some DNS servers' query responses may originally suggest a time-to-live (TTL) for cached results that is too long and wastes RAM, or you may have recently changed DNS records and need to force them to take effect immediately. Previously, you could flush the entire cache. Now, alternatively you can now set a maximum age for cache entries.

Feature	Description
AES-GCM support for S/MIME	AES-GCM cipher support has been added for S/MIME.
Support country exclusion in GeoIP Group	Added a configurable exclusion list under *Profile* > *Group* > *GeoIP Group*.
Email archive enhancement	Added option to repackage original email as attachment in archive account settings.
Access FortiSandbox verdict details directly from FortiMail	When the classifier is 'FortiSandbox File', FortiSandbox report can be downloaded by right clicking the history log.
Allow admin users with read/write access to restore a firmware image	When configuring an admin profile, a Firmware Update option is available under System > Maintenance if the admin user is granted read/write permissions.

GUI

Feature	Description
Recent email statistics and log dashboard	Recent Email tab on the dashboard will display when at least one of the following settings is enabled: Delivery Status, TLS Tracking, or the mailstat-service CLI global setting.
New fields in history logs	Added "Display Name" and "Reply To" to history logs.
Expose CDR component types on GUI	The Microsoft Office and PDF attachment component types to be disarmed are now configurable under *Security* > *Disarm & Reconstruction* > *Attachment*.

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.
FortiIsolator removal	Removed integration with FortiIsolator in content disarm and reconstruction (CDR) settings.
Moved some CLI only settings to GUI	• Some safe/block list and QR code scan CLI only settings under "config antispam settings" are made available on the GUI under relevant menus. • Attachment content types to be disarmed under "config file content-disarm-reconstruct" are made available under *Security* > *Disarm & Reconstruction* > *Attachment* on the GUI.

DKIM body length tag	Honoring the DKIM body length tag (l=) means to checks only the specified number of bytes or characters in the email body rather than the whole message.
	FortiMail's default behavior is to honor the tag.
	Starting from v8.0.2, the following CLI command has been added to ignore the tag. For better security, RFC 6376 recommends that you disable this setting.
	`config antispam settings`
	`  set dkim-honor-body-length {enable|disable}`
	`end`

Auth password length limit	Reduced from 139 to 98 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
1307581	After upgrading to FortiMail 8.0.0, some legitimate emails are modified by Content Disarm and Reconstruction (CDR) and some CDR settings cannot be saved.
1265528	QR code with 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.
1319365	In some cases, duplicate emails are released from the system quarantine.
1351218	Delivery issue caused by long domain names.

System

Bug ID	Description
1313784	CA issuer validation fails when the issuer DN contains "/" characters.
1309261	Incorrect time zone for Vilnius.

Bug ID	Description
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.
1290973	TLS signature algorithm still accepts SHA224 / DSA family.
1287360	After upgrading from FortiMail 7.2.x to v7.4.x or v7.6.x, domain-level RADIUS profiles stop working.
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
1284629	If an image is detected as image spam, there are no details in the logs about which image is detected if there are multiple image files.
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.
1288828	Sent folder issue after email migration.
1297833	After upgrading from FortiMail 7.6.4 to v8.0.0, search in the dictionary profile stops working.
1293895	After upgrading from FortiMail 7.6.4 to v8.0.0, file signature lists are missing.
1290547	After upgrading from FortiMail 7.6.4 to v8.0.0, greylist exempt lists are missing.
1323501	Cyrillic character display issue.

Bug ID	Description
1291585	After upgrading from FortiMail 7.6.4 to v8.0.0, some dashboard settings are missing and widget positions are reset.
1298828	Webmail sent folder email display issue after mail migration.

Common Vulnerabilities and Exposures

FortiMail 8.0.2 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1303920 1303439 1348679 1335851 1336260 1335852	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
1303443	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
1320714	CWE-321: Use of Hard-coded Cryptographic Key
1324042	CWE-522: Insufficiently Protected Credentials
1318177	CWE-1050: Excessive Platform Resource Consumption within a Loop

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) > **8.0.2** (build 263)

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 8.00015

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.