Release Notes

FortiMail 8.0.0

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 05, 2026
FortiMail 8.0.0 Release Notes
06-800-1277272-20260505

TABLE OF CONTENTS

Change log **4**
Introduction and supported models **5**
Supported models 5
What's new **6**
Antispam/Content 6
GUI 7
System 7
What's changed **9**
Special notices **10**
Communication between HA secondary units 10
HA heartbeat and DHCP 10
TFTP firmware install 10
Firmware upgrade and downgrade **11**
Upgrade path 11
Firmware downgrade 11
Firmware image checksums 11
Product integration and support **13**
FortiNDR integration 13
FortiIsolator integration 13
FortiAnalyzer Cloud integration 13
AV engine 13
Recommended browsers 13
Resolved issues **15**
Antispam/antivirus 15
Email delivery 16
System 17
Log and report 18
Administrator GUI/webmail 18
Common Vulnerabilities and Exposures 19
Known issues **20**

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
2026-05-05	Initial release of the FortiMail 8.0.0 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 8.0.0 feature release, build 183.

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, 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 • Nutanix AHV

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.

Antispam/Content

Feature	Description
Microsoft 365 Inline Scan	Use Microsoft Exchange Online connectors and rules to route internal/inbound/outbound emails from Microsoft 365 to FortiMail for scanning.
Microsoft 365 Shared Mailbox Scan	Scan shared mailboxes in Microsoft 365 for accounts with sign-in blocked.

Option to Send Notification via FortiMail MTA in Microsoft & Google API Mode	When FortiMail runs in Microsoft & Google API mode, customization of the header `From:` field in the notification email templates is not supported by default.
	Use the following CLI command to change the behavior:
	`config cloud-api setting`
	`set notify-method {api | smtp}`
	`end`
	• `api`: Default setting. Notifications will be sent by MS365 API. The customized email `Subject` will be applied but the header `From:` will be kept.
	• `smtp`: Notifications will be sent by FortiMail MTA (SMTP). Both the customized email `Subject` and header `From:` will be applied.

Password-protected Attachment Scan	Prompt the user for a password before scanning a password-protected attachment.
QR Code in PDF Archives	Scan QR code URL in PDF archives.
Quarantine Release Rescan	Under *Security* > *Quarantine* > *Quarantine Control*, there are now settings to re-scan email with content and DLP scans when the email is released from quarantine.
Office File Metadata and HTML Hidden Content Handling	CDR settings in content profiles can now be used to retain or remove Microsoft Office file metadata and HTML hidden content, such as transparent, hidden, or tiny images and text that are hard to see.
Access Control with From:	(Advanced management license required) Added the following CLI setting in access control receive policies to select whether to match the sender email address in the SMTP envelope (`MAIL FROM:`), message header (`From:`), or both. Default setting is `envelope-from`.

Feature	Description
	config policy access-control receive edit <rule_id> set sender-option {envelope-from | envelope-or-header-from | header-from} end
Safelisting with Reply-To:	The Reply-to: message header can now be used with the safe lists. config antispam setting set safelist-check-reply-to {enable | disable} end

GUI

Feature	Description
New Administrator GUI	New framework for the administrator GUI.
Support SAML SSO with Separate SP for Webmail	Separate the SAML SSO SP setting so that the webmail and administrative GUI can be distinguished separately on the IdP.
2FA Integration with FortiIdentity Cloud	Multi-factor authentication (MFA) tokens with FortiIdentity Cloud (formerly FortiToken Cloud) can now be used for administrator accounts.
Client IP Address from X-Header	HTTP X-headers can now be used to identify the original client IP address under *System* > *Configuration* > *Web Service*. This is useful when there is an upstream proxy or load balancer that is not transparent, and therefore the original client's IP address is not directly visible for features such as repeat offender control.
Unreleased /Released Quarantine Count	Message counts for email that are released or not released from the quarantine are now shown under *Monitor* > *Quarantine*.
Disk Usage History	Disk usage history is now in a widget on the dashboard.
TLS Connection Statistics	TLS statistics are now included under *FortiView*.

System

Feature	Description
Personal Block/Safe List Size Limit and Tracking	(Advanced management license required) Control personal block/safe list size and display the usage information under *Security* > *Block/Safe List* > *Personal*.
Sender Exclusion	Sender exclusion can now be configured in recipient-based policies.

Feature	Description
Secure RADIUS	RADIUS profiles now support secure (TLS) RADIUS.
SNMPv3 Enhancement	Added support for SNMPv3 authentication with SHA256/SHA384/SHA512 and privacy (encryption) with AES256 under *System* > *configuration* > *SNMP* > *User*.
Archive Action in Microsoft & Google API Mode	Archive action is now supported in Microsoft & Google API mode.
Disclaimer Enhancement	Mobile devices' banner notifications for new email may include a preview of the start of the email.To avoid including the disclaimer in the preview, there are now options to convert plain text to HTML email, and for HTML email, to hide the disclaimer in the preview.
Regex Support in Header Manipulation	Regular expressions can now be used in header manipulation in session profiles.
Mail Delivery Status	New delivery status, "Delivering", is now used. Also added the failure reason if the delivery failed.
Mail Delivery Status on FortiAnalyzer	Store and update the delivery status on FortiAnalyzer.
SED Drive Auto Lock	Enable use of the MegaRAID SafeStore "Auto Lock" feature of the RAID controller with self-encrypting drives on the FML-900G model.
Remote Email Archive Port Number	Port numbers are now configurable with the host name for remote email archive servers.
FortiAuthenticator Integration	(Server mode only) FortiMail can now connect to FortiAuthenticator for remote management of user accounts. This is useful in large deployments, so that you do not need to leave the FortiMail administrator GUI in order to create, update, delete, import, or export accounts that are stored remotely on FortiAuthenticator.

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
Stronger Local Password Encryption at Rest	Passwords for FortiMail administrators that use local authentication are encrypted when stored in the configuration file. FortiMail 8.0.0 now offers stronger encryption at rest. When each administrator logs in, their password will be automatically migrated to the new encryption format. Alternatively, the `admin` account or another super administrator can reset all passwords so that FortiMail immediately uses the new format for all local administrator accounts. **Caution:** If you are temporarily testing the new firmware, then passwords **must** be stored in both the new and old format. Otherwise when you downgrade, administrators may not be able to log in. This could require a clean install and recovery from a backup.
Case-insensitive Administrator Names	Names in administrator login dialogs are now case-insensitive. Previously, names were case-sensitive. **Note:** When you upgrade to FortiMail 8.0.0 or later, if some names differ only by capitalization, they are automatically renamed so that they will still be uniquely identifiable. For example, `admin` and `Admin` could be renamed to `admin` and `Admin_1`. To find renamed administrator accounts, see the log messages.
Firmware Management	Added a firmware tab under *System* > *Maintenance* > *Firmware* for administrators to update the firmware and view the update history.
Simplified Mail Statistics Reports	Query names and time periods are now simpler. Some bugs were fixed. **Note:** Default values have changed. This may mean that reports are automatically generated at a different time, or include different charts and intervals. When you save a report profile, settings in the configuration file will be migrated to their new equivalents.
Dedicated Antispam Setting Page	Moved the *AntiSpam* section under *Security* > *Option* > *Preference* to *Security* > *Option* > *AntiSpam*.
Session Profile Wording and Layout Changes on the GUI	Reorganized the GUI sections and changed some wording.
CLI Command Relocation	Many CLI settings have been moved or renamed. For details, see the change log in the FortiMail CLI Reference.
Event Time in Milliseconds in Logs	To accommodate FortiAnalyzer requirements, `eventtime` in FortiMail logs are now in milliseconds.

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) > **8.0.0** (build 183)

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

AV engine

- Version 8.00015

Recommended browsers

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

- Google Chrome 147
- Microsoft Edge 147
- Mozilla Firefox 150
- Apple Safari 26

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
1165264	Embedded URLs in PDF attachments were not detected.
1172602	EMF files were incorrectly detected as `application/zip`.
1184804	Wrong MIME type detection.
1183090	JPEG image files were incorrectly detected as RAR files.
1200245	When sender address rate control reached the limit and some email are in the FortiSandbox queue, FortiMail received `No Result` from FortiSandbox.
1191454	Replacement message action in the content profile action did not work properly.
1194912	SPF checks failed if there were unknown modifiers.
1189764	Decompressed large files were not scanned or sent to quarantine.
1190142	Content type was changed although *Deliver to original host* was set to *Unmodified copy*.
1199314	URLs in invisible HTML text were not scanned.
1203450	Antispam IP reputation did not work after FortiSandbox was disabled.
1227717	More variables were needed in the password protected attachment notification email template.
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.
1217422	After an upgrade from FortiMail 7.6.3 to 7.6.4, if re-scan upon quarantine release was enabled, email in personal quarantines could not be release.
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.

Bug ID	Description
1240477	URI redirect lookup did not work properly.
1244117	Content action in policy matches should have been classified as `Not spam` instead of `Spam`.
1244705	Password-protected attachment notifications should have appeared at the top of the email, not the bottom.
1253486	URLs with hyphens in PDF attachments were not parsed properly.
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.
1286724	ZIP files containing BAT files were not detected by the content filter.
1283521	Newsletter is not detected if FortiMail performs 'Expanding alias' based on the LDAP profile query.

Email delivery

Bug ID	Description
1191404	Missing header "From:" value.
1180692	Error messages occurred when clicking the encrypted email notification link if the email had been filtered by other security solutions.
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.

System

Bug ID	Description
1164834	After an upgrade to FortiMail 7.6.3, the HA group was out of synchronization.
1209753	High CPU usage was caused by DLP profiles.
1173175	Legitimate email was caught by intelligent analysis.
1182035	In some cases, while in HA mode, a block list entry could be missing
1195444	When FIPS-CC mode is enabled, LDAPS must disable the use of algorithms and TLS versions that are not FIPS-approved and certified.
1198879	When FIPS-CC mode is enabled, IBE, S/MIME, and SNMPv3 must disable the use of algorithms that are not FIPS approved and certified..
1181436	Some disclaimer variables did not work properly.
1161849	After an upgrade from FortiMail 7.4.3 to 7.6.3, the system crashed intermittently. The error message was: `Failed to boot default entries.`
1189164	Calendar sharing did not work for Microsoft Outlook.
1181505	High CPU usage occurred in some cases.
1197184	Changing banned words or dictionary profiles did not work properly.
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.
1260258	In some cases, quarantine release notification confirmation did not show the password input field.
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.
1098759	After an upgrade to FortiMail 7.6.0 or 7.6.1, address books disappeared.
1183070	Unable to add line break/carriage return in replacement messages.
1282440	Address map rewriting did not comply with RFC 2047 encoding for Cyrillic display names.

Log and report

Bug ID	Description
1195458	Log reports with a comma in their name could not be generated or deleted.
1248953	After an uprade to FortiMail 7.6.4, regular expression errors were logged on every SSH login.
1168320	In antispam logs, the error message `database error executing` could appear.
1232787	File names were not displayed correctly in logs.
1260702	Tables were truncated in downloaded PDF reports.

Administrator GUI/webmail

Bug ID	Description
1198315	Updated the JQuery-UI version.
1176950	Under *Security* > *URL Filter* > *Profile*, the total number of references did not display correctly.
1196837	In ForitMail webmail, encrypted email for Zoom session links was replaced with ICS file attachments.
1194351	Character T and Z appear in FortiMail clawback timestamp for the personal quarantine report email template.
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.

Common Vulnerabilities and Exposures

FortiMail 8.0.0 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
1169607	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')
1202972	CWE-358: Improperly Implemented Security Check for Standard
1286744	CWE-472: External Control of Assumed-Immutable Web Parameter
1202972	CWE-358: Improperly Implemented Security Check for Standard
1173144	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere

Known issues

No known issues.

www.fortinet.com