Release Notes

FortiMail 7.4.4

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

August 29, 2025
FortiMail 7.4.4 Release Notes
06-744-1130305-20250829

TABLE OF CONTENTS

Change Log **4**
Introduction and Supported Models **5**
Supported models 5
What's New **6**
What's Changed **7**
Special Notices **8**
Communication between HA secondary units 8
HA heartbeat and DHCP 8
TFTP firmware install 8
Monitor settings for the GUI 8
SSH connection 9
FortiGuard web filtering category v10 update 9
Product Integration and Support **10**
FortiNDR support 10
FortiIsolator support 10
FortiAnalyzer Cloud support 10
AV Engine 10
Recommended browsers 10
Firmware Upgrade and Downgrade **11**
Upgrade path 11
Firmware downgrade 11
Resolved Issues **12**
Antispam and Antivirus 12
IBE and S/MIME 13
System 13
Log and Report 13
Administrator GUI and Webmail 14
Common Vulnerabilities and Exposures 14

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
2025-02-27	Initial release of FortiMail7.4.4Release 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 7.4.4 mature release, build 607.

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.

Feature	Description
Logs for users moving email in Microsoft 365 and Google API view	When a user discards or manually moves an email to the personal or system quarantine, inbox, or other folder via the Microsoft 365 or Google API view, the event is now logged.

What's Changed

The following table summarizes the behavior and GUI changes in this release.

Feature	Description
Log the IP address for password changes	When an administrator or user updates their password, the system event log now includes the IP address where the change was requested from.
Multi-line log messages	Log messages for configuration changes include a list of changes. Before, a long list of changes might exceed the limit of 64 characters, resulting in a truncated log message. Now, log messages may use multiple lines, and can show the complete change.

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.

Monitor settings for the GUI

To view all objects in the GUI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280 x 1024.

SSH connection

For security reasons, starting from FortiMail 5.4.2, FortiMail does not support SSH connections with plain-text password authentication. Instead, a challenge/response should be used.

FortiGuard web filtering category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency web sites. In order to use the new categories, customers must upgrade their Fortinet products to one of the versions below.

- FortiMail 7.0.7, 7.2.5, 7.4.1 or later

Product Integration and Support

FortiNDR support

- Version 7.0.0

FortiIsolator support

- FortiIsolator 2.3 and later

FortiAnalyzer Cloud support

- Version 7.0.3

AV Engine

- Version 6.00297

Recommended browsers

For desktop computers:

- Google Chrome 134
- Mozilla Firefox 135
- Microsoft Edge 133
- Apple Safari 18

For mobile devices:

- Official Google Chrome browser for Android 15
- Official Safari browser for iOS 18

Firmware Upgrade and Downgrade

Before any firmware upgrade or downgrade, save a copy of your FortiMail configuration by going to *Dashboard* > *Status* and click *Backup* in the *System Information* widget.

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 GUI screens. Also go to verify that the build number and version number match the image loaded.

The 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) > **7.4.4** (build 607)

Firmware downgrade

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

- operation mode
- network interface IP address or management IP address
- static route table
- DNS settings
- administrator accounts
- administrator access profiles

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 and Antivirus

Bug ID	Description
1075043	For the system quarantine, alphabetical sort ordering for the Ukrainian alphabet was not correct for some characters.
1082373	With FortiSandbox, high CPU usage and delayed mail could occur with heuristic and QR code scans.
1082843	When upgrading the FortiGuard Antivirus database, `smtpd` may terminate.
1090327	A DMARC report is not generated when the domain name for the RUA `mailto` does not match the sender domain.
1094034	In some cases, if the DMARC alignment check fails, then the DMARC check still will not fail.
1098766	With FortiSandbox, phishing URLs with specific character combinations are not caught.
1100041	In Gmail, quarantine reports could not use the webmail method to release or delete email.
1100219	Some URLs in an email may not be submitted to FortiSandbox.
1104413	High CPU usage by mailfilterd could occur with some PDF attachments.
1107735	Some attachment file names cause email with an empty recipient that cannot be released from the system quarantine.
1111258	In DLP rules, a regular expression match all condition does not function correctly if both *Body* is empty and *Subject* is empty.
1111271	Dictionary profile names may remain after restoring an older configuration that does not contain the profiles.
1119288	For dictionary scans with regular expressions, valid patterns sometimes did not match UTF-8 encoded subject lines.
1115693	When creating a scheduled scan in the Microsoft 365 API view, the advanced condition is ignored.
1121575	When a ZIP file is password-encrypted but the content profile does not have the password, sometimes FortiMail does not quarantine the file as expected, but instead submits it to FortiSandbox. This causes an error log on FortiSandbox: `WARNING: Wrong password for file submission`
1128095	When uploading a safe list or block list via the REST API, it could fail with the error message `Access Check Failed`

IBE and S/MIME

Bug ID	Description
1086810	In some cases, the URL for IBE password reset or reactivation incorrectly gives an HTTP `403 Forbidden` permissions error.
1110089	For email clients that use the RSA-OAEP key exchange algorithm, the recipient is unable to decrypt the email. Antispam logs show the error message `DecrypterMediaIn: Decoded Data not valid`.

System

Bug ID	Description
1029391	Outgoing mail queues sometimes may grow and become slow to deliver, clear, or display on the GUI.
1069702	For FortiGate Security Fabric communications, FortiMail broadcasts destination port number 8014 to the wrong IP address.
1076001	Some SSH key exchange algorithms should be removed when strong cryptography is enabled.
1087752	In active-active mode with HA, SNMP OIDs `fmlHAEffectiveMode` and `fmlHAMode` show the wrong roles.
1094863	In alert email, a recipient with an internal domain could not be added due to strict domain checking.
1103297	When a user with the same name exists in an LDAP directory, a new user could not be created locally.
1107717	`remote_wildcard` administrators have permissions to create administrator accounts, but cannot delete them.

Log and Report

Bug ID	Description
1078550	Quarantine reports may be garbled when special characters are used in the email subject and `remove-active-content` is enabled.
1089762	Scheduled reports are delivered later than expected.
1105759	Log message `Timed out checking block safe lists` is misleading.
1114308	For domain-level administrators, searching the logs may show sometimes show results from other protected domains.

Administrator GUI and Webmail

Bug ID	Description
1101465	In some cases, HTML email is not displayed properly.
1115801	Webmail session timeout does not respect the idle timeout setting.

Common Vulnerabilities and Exposures

FortiMail 7.4.4 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1071459	CWE-: Stack-based Buffer Overflow
1092958	CWE-23: Relative Path Traversal

www.fortinet.com