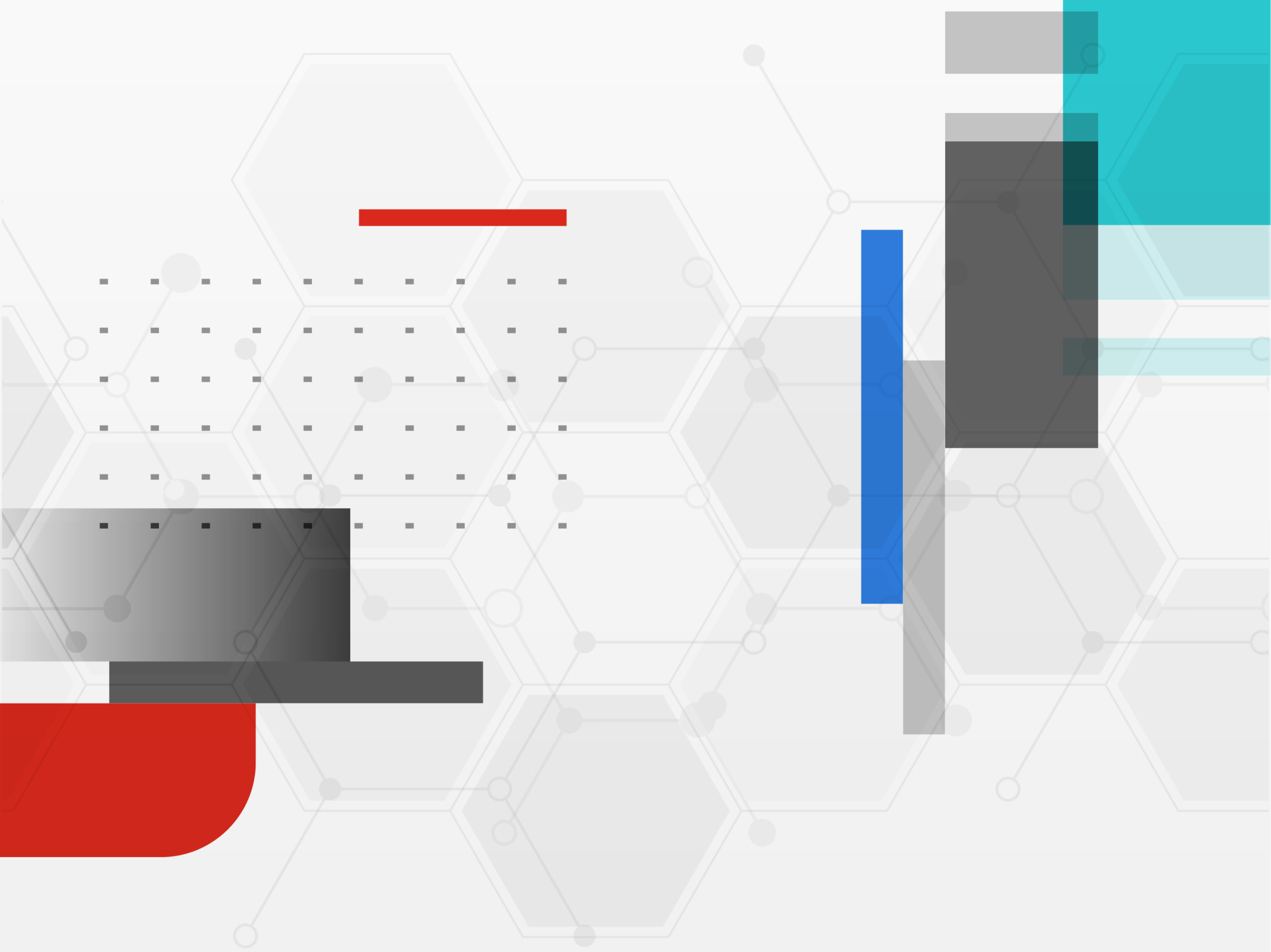
Release Notes

FortiMail 7.4.6



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

December 11, 2025
FortiMail 7.4.6 Release Notes
06-746-1235575-20251211

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
2025-12-11	Initial release of FortiMail 7.4.6 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 7.4.6 mature release, build 620.

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 • Azure BYOL • Google Cloud Platform BYOL • Oracle Cloud Infrastructure BYOL

What's New

None.

What's Changed

None.

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

Recommended browsers

For desktop computers:

- Google Chrome 144
- Mozilla Firefox 145
- Microsoft Edge 143
- 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.

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) > **7.4.6** (build 620)

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/antivirus

Bug ID	Description
1165264	Embedded URLs in PDF attachments are not detected.
1172602	Files with .emf extension are incorrectly detected as application/zip files.
1163240	Email with image attachment is blocked by the content profile as password-protected file.
1184804	Wrong MIME type detection.
1183090	JPEG files are incorrectly detected as RAR files.
1200245	When sender address rate control reaches the limit and some email are in the FortiSandbox queue, FortiMail receives NoResult from FortiSandbox.
1191454	Replacement message action in the content profile action does not work properly.
1194912	SPF check fails due to unknown modifiers.
1189764	Decompressed files with big size are not scanned or sent to quarantine.
1190142	Content type is changed although "Deliver to original host" action is set as "Unmodified copy".
1213884	URL click protection may not work properly during heavy workload.
1189587	"UNSEEN" error message returned from FortiSandbox.

Email delivery

Bug ID	Description
1191404	Need to add missing header "From:" value.

System

Bug ID	Description
1160450	When generating a certificate signing request (CSR), FortiMail does not add the X509v3 Subject Alternative Name (SAN) extension to the request.
1164834	After upgrading to v7.6.3 release, the HA pair is out of synchronization.
1209753	High CPU usage caused by DLP profiles.
1173175	Legitimate email caught by Intelligent Analysis.
1182035	In some cases, a block list entry may be missing in HA mode.
1195444	For FIPS-CC purpose, LDAPS needs to drop the non-approved and non-certified algorithms / TLS versions.
1198879	Disabling use of non-FIPS approved algorithms in IBE, S/MIME, and SNMPv3.
1181436	Some disclaimer variables may not work properly.
1161849	After upgrading v7.4.3 to v7.6.3, the system began crashing intermittently with the error message: Failed to boot default entries.
1189164	Calendar sharing does not work for Microsoft Outlook.
1223903	On some lower FortiMail models, PDF scanning may cause high CPU and memory usage.
1220666	High CPU usage caused by PDF attachments.
1156491	DKIM keys may be lost from the configuration.

Log and report

Bug ID	Description
1168320	Database error executing message in antispam logs.
1232787	In some cases, the logs may not show the correct attachment file names.

Administrator GUI/webmail

Bug ID	Description
1198315	Updated the JQuery-UI version.

Bug ID	Description
1176950	Under Security > URL Filter > Profile, the total ref number does not display correctly.
1196837	In ForitMail webmail, encrypted email for Zoom session links is replaced with .ICS file attachment.
1194351	Character T and Z appear in FortiMail clawback timestamp for Quarantine Summary email template.
1173729	In server mode, the secondary identify cannot be deleted in the user preference.
1054198	In some cases, quarantine search may not work properly on the HA primary unit.
1189608	In some cases, personal quarantine search may not work properly.

Common Vulnerabilities and Exposures

FortiMail 7.4.6 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
1173145	CWE-312: Cleartext Storage of Sensitive Information
1173144	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere
1169607	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
1234022	CWE-121: Stack-based Buffer Overflow
1233871	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Known Issues

None.

www.fortinet.com