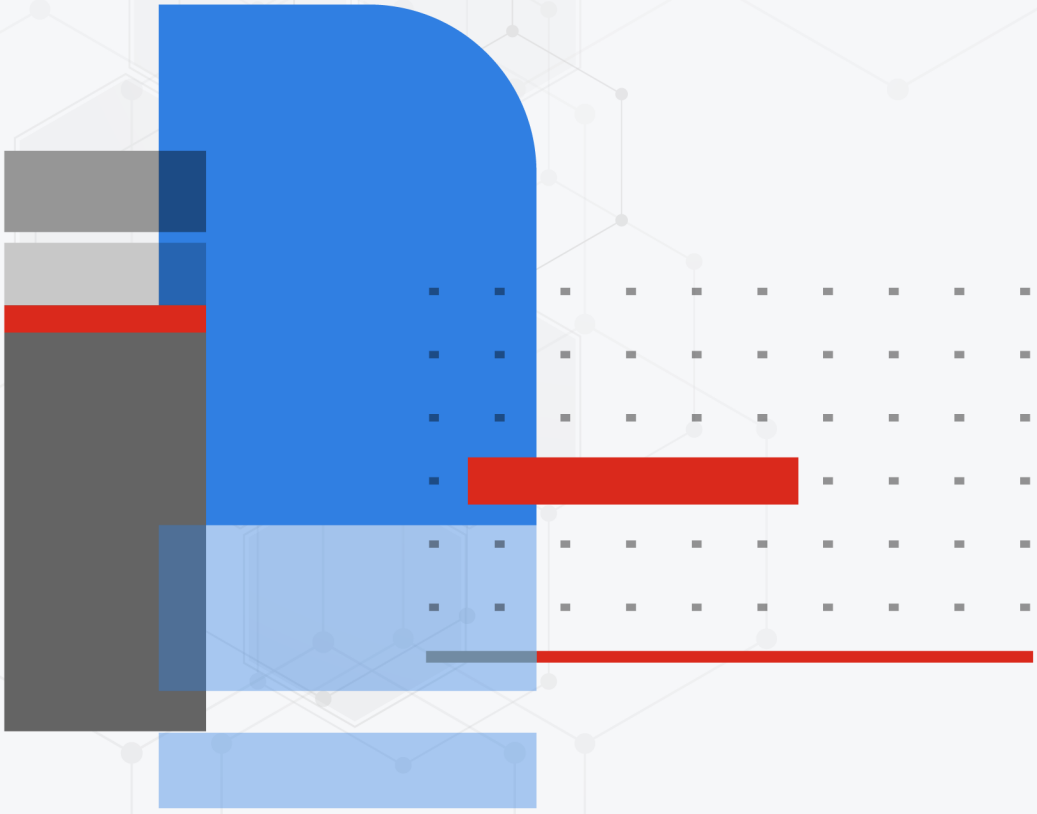
Release Notes

FortiMail 7.4.3



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 21, 2024
FortiMail 7.4.3 Release Notes
06-743-1065796-20240821

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-08-21	Initial release.

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 7.4.3 mature release, build 600.

For FortiMail documentation, see the Fortinet Document Library.

Supported models

FortiMail	200F, 2000E, 2000F, 3000E, 3000F, 3200E, 400F, 900F
FortiMail VM	• VMware vSphere Hypervisor ESX/ESXi 7.0, 8.0 and higher • Microsoft Hyper-V Server 2016, 2019, and 2022 • KVM qemu 2.12.1 and higher • Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher • 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
SSO Enhancement	Support dynamic IP addresses within the same SAML session.
IBE 2FA Local Gateway Service	Support United Arab Emirates (UAE) local SMS gateway Etisalat for IBE 2FA.

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.

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 web UI

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

SSH connection

For security reasons, starting from 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, 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 - Fixed in 7.0.7, 7.2.5, 7.4.1.

Product Integration and Support

FortiNDR support

- Version 7.0.0

FortiIsolator support

- FortiIsolator 2.3 and above

FortiAnalyzer Cloud support

- Version 7.0.3

AV Engine

- Version 6.00297

Recommended browsers

For desktop computers:

- Google Chrome 127
- Firefox 127
- Microsoft Edge 127
- Safari 17

For mobile devices:

- Official Google Chrome browser for Android 12 and 13
- Official Safari browser for iOS 16 and 17

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 web UI 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 AV 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)

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

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
1013426	URL click protection is triggered even if the URL doesn't match the URL rewrite category.
1011714	URL is not rewritten although the log shows otherwise.
1015911	In some cases, URLs are incorrectly removed.
1004244	Fails to parse Base64 escaped UTF-8 strings.
1026973	In some cases, domain block list entry for *@* is added automatically.
1054713	No DKIM signing for S/MIME outbound mail.
1034037	QR codes are not detected in the email body and the attachment .jpg or .png files.
1040094	In some cases, URL removal may render the email unreadable in the system quarantine.
1036933	Email may reach one recipient but not another due to incorrect DMARC checking.
1031454	DLP rule won't be triggered for Arabic PDF 1.4 files.
1060851	DMARC check fails because the DKIM signature passes and fails for the same record.
1016396	QR code with logo inside cannot be detected.

Mail Delivery

Bug ID	Description
1002178	When LDAP mail host attribute is empty/unavailable, the domain setting should be used for mail delivery.

System

Bug ID	Description
1020012	Extended DSN does not work.
1019843	In some cases, not all sender rate control notifications are sent.
1016312	Some sender rate control notification email contents are blank.
1011246	IBE reactivation notification uses wrong Mail From address.
926899	Fails to respond to IPv6 requests in some cases.
1009303	MTA-STS policies cannot be matched properly.
1057857	Maximum value of IP address groups was lowered incorrectly for MSSP licenses.
1009074	Virtual IP stopped working in HA cluster after upgrading from v7.2.5 to v7.4.1.
1049367	In some cases, FortiMail-900F CPU usage may increase intermittently.
1012948	No search result for quarantined messages.
1039017	In a recipient policy, changes to "Email address group" recipient pattern are not saved.
1036907	FortiMail interface MAC addresses are inconsistent with ESXi VM NICs MAC addresses after adding the 5th interface to the VM.
1039434	"dsn-ehlo-other-name" does not display in mail header.
1033072	Upgrading to 7.2.6 causes issue with interface link status.
1017957	After upgrade from v7.2.5 to v7.4.2, IP pools become unavailable.
1010217	If an administrator accidentally disables the last admin account, there is no way to log in to FortiMail anymore.
1019309	IPv6 virtual IP does not work properly on HA fail-over.
1026933	SHA256 is not supported for S/MIME signing.
1015411	RADIUS authenticated accounts cannot see "Archive to account" action in all action profiles.
1006058	After upgrading from v7.2.4, to v7.4.2, administrators cannot log in to FortiMail with FortiAuthenticator using the remote_wildcard user.
1962734	In some cases, users cannot add new entries to the block/safe Lists.
1063389	FortiMail VM does not launch with IMDSv2 (token required) configuration on AWS EC2.
1061797	SMIME does not work properly with Cisco Mail Gateway.
1034247	High CPU usage when receiving some specific files.

Log and Report

Bug ID	Description
1012390	TLS minimum version enforcement log is incomplete.
1001596	Mail statistics report doesn't work as expected when there are multiple-level protected domains.
1022958	CDR logging enhancement.
1035752	In some cases, the miglogd daemon may get stuck and cause failure to send logs to FortiAnalyzer Cloud.
1021029	Mail Filtering Statistics "both directions" report does not add up the incoming and outgoing statistics reports.
1012298	In HA mode, log search results on the primary unit are not displayed correctly when logs are pushed back from the secondary units.

Admin GUI/Webmail

Bug ID	Description
1006119	When filling the name in the "To" filed that contain Cyrillic, the results are not displayed correctly.
987280	Scroll bar does not show when trying to switch users in webmail.
1022492	In some cases, adding comments with spaces may cause the system to reboot.
1052300	Error "Entry is not found" occurs when copying the content profile.
1018416	Bayesian training page does not update properly.
1050096	Admin GUI does not show inbox subfolders created by email user.
1027854	If the recipient display name contains an apostrophe, the email is not sent to this recipient.
1040096	Newly created DKIM key does not show up on the GUI promptly.
1014451	Cannot handle Cyrillic symbols properly in the To fields in webmail.
998632	Webmail SSO users will not be logged out after idle time.
1007457	VLAN Interfaces are not displayed on HA configuration GUI.
1001552	Under Profile > Content > File Password, editing a password comment fails with error.
1022492	In some cases, adding comments with spaces may cause the system to reboot.
1068718	The webmail login portal does not work with the customized template.

Common Vulnerabilities and Exposures

FortiMail 7.4.3 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1051927	CVE-2024-6387: regreSSHion: RCE in OpenSSH's server, on glibc-based Linux systems
1001069	CWE-602: Client-Side Enforcement of Server-Side Security
1033933	CWE-613: Insufficient Session Expiration
1057581	CWE-201: Insertion of Sensitive Information Into Sent Data

www.fortinet.com