FortiMail - Release Notes

Version 6.4.7

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 21, 2022
FortiMail 6.4.7 Release Notes
06-647-826175-20220721

TABLE OF CONTENTS

Change Log **4**
Introduction and Supported Models **5**
Supported models 5
Special Notices **6**
TFTP firmware install 6
Monitor settings for the web UI 6
SSH connection 6
Product Integration and Support **7**
FortiSandbox support 7
AV Engine 7
Recommended browsers 7
Firmware Upgrade and Downgrade **8**
Upgrade path 8
Firmware downgrade 8
Resolved Issues **9**
Antispam/Antivirus 9
Mail delivery 9
System 10
Log and Report 11
Admin GUI and Webmail 11
Common Vulnerabilities and Exposures 11
Known Issues **12**

Change Log

Date	Change Description
2022-07-21	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 6.4.7 release, build 467.

Supported models

FortiMail	60D, 200E, 200F, 400E, 400F, 900F, 1000D, 2000E, 3000E, 3200E
FortiMail VM	• VMware vSphere Hypervisor ESX/ESXi 6.0, 6.7, 7.0 and higher • Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2, 2016 • KVM qemu 2.12.1 and higher • Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher • AWS BYOL • Azure BYOL • Google Cloud Platform BYOL

Special Notices

This section highlights the special notices that should be taken into consideration before upgrading your platform.

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 1280x1024.

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.

Product Integration and Support

FortiSandbox support

- FortiSandbox 2.3 and above

AV Engine

- Version 6.2.167

Recommended browsers

For desktop computers:

- Google Chrome 103
- Firefox 102
- Microsoft Edge 103
- Safari 15

For mobile devices:

- Official Google Chrome browser for Android 12
- Official Safari browser for iOS 15

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

Any 4.x release older than **4.3.6** > **4.3.6** (build 540) > **5.2.3** (build 436) > **5.2.8** (build 467) > **5.3.10** (build 643) > **5.4.4** (build 714) (required for VMware install only) > **5.4.6** (build 725) > **6.0.5** (build 148) > **6.2.4** (build 272)> **6.4.7** (build 467)

When upgrading from 6.2.7 to 6.4 release, you must upgrade to 6.4.5 and newer releases, not other older 6.4 releases.

Firmware downgrade

Firmware downgrading is not recommended and not supported in general. If you need to perform a firmware downgrade, follow the procedure below.

1. Back up the 6.4.7 configuration.
2. Install the older image.
3. In the CLI, enter `execute factoryreset` to reset the FortiMail unit to factory defaults.
4. Configure the device IP address and other network settings.
5. Reload the backup configuration if needed.

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
784305	HTML file passed content filter profile set to block *.html files.
783166	SPF check fails for Microsoft 365 API mail.
782699	Content profile scanning proceeds even after final quarantine action is triggered.
782367	DLP configuration not blocking empty pages as expected.
773494	MIME header can be manipulated to bypass antivirus scanning.
770445	DLP not detecting words in headers and footers of Microsoft Word documents.
770841	URL exemption for domain name not working with uri-checking set to "aggressive".
770566	Malicious URI in text format bypassing FortiGuard URL filter check.
797391	CDR feature URL click protection not working correctly with rewrites not occurring for URLs within emails.
803094	Content filter with wildcard patterns cannot detect Thai language.
800994	Outbound emails rejected due to timeout while logs display (Disposition: Accept).
815586	FortiSandbox category timed out, with action taken before timeout was triggered.
827697	Email address starting with "."(dot) is not rejected.

Mail delivery

Bug ID	Description
785327	DKIM check failed due to public key being invalid or irretrievable.
774758	Undeliverable NDR resent without following the mail routing profile.
773010	Bounce verification scan not removing verified tags.
819657	The "for" clause in the Received Header contains another recipient address when Spam outbreak is triggered.

System

Bug ID	Description
786272	Disclaimer not added even when "insert disclaimer" was enabled.
778938	"Attempt to decrypt archive" and "Words in e-mail content" not decrypting .zip files.
672299	The dnscached process became corrupted during periods of heavy traffic.
770190	DKIM check failed due to signature for domain being invalid.
772318	Push update not working as expected.
770916	Unable to configure distinguished names (DN) with more than a 127 character length.
766819	Mail data corrupted when transferred to NAS device.
788629	Associated domain should use the primary domain Bayesian database.
794074	SSO administrator login not working when post-login-banner is enabled.
781108	High memory usage exhibited from primary node due to hasync process but not processing any mail.
807614	DKIM keys from some domains are missing.
799789	Invalid DKIM signature issue.
798144	Issue when System Time is set to use GMT time zone.
797330	Disclaimer being added in emails in the incorrect place.
815286	SPF check receives PERM_ERROR message when sender record includes macros and IPv6 client IP .
692481	Custom email template variable %%ORIG_FROM%% not working as intended.
811593	Attachment scan action with two file filters stops with replace action.
811446	Scheduled Scan set to "daily" is defaulting to 24-hour window instead of the shorter time period configured.
810685	Using FortiMail in Server mode withLDAP server, unlike local users, LDAP users are unable to delete user mailbox data.
824290	Disclaimer duplicate stamping issue.
824015	SPF check failed due to DNS look up limit reached.
822265	DKIM check failed due to body hash being invalid.
818908	Content Disarm and Reconstruction URL not working.
819717	Disclaimer not being added to all emails.
826087	FortiMail detects .jtd files as Microsoft files.
817272	Issue with HA synchronization due to certificate checksum mismatch.

Log and Report

Bug ID	Description
786675	System event logs were not generated when either creating or deleting DKIM key pairs.
781956	User safe and block list additions via webmail missing from System Event log.
797621	Log search not working correctly, giving message "Done with exception".

Admin GUI and Webmail

Bug ID	Description
777084	Sender Reputation search filter not working with Relationship set to "OR".
764729	FortiMail VM in Server mode with "Failed to open mailbox" error.
768328	Per sub-domain administrators cannot see domains in gateway mode.
804163	Incorrect translation to Japanese of "Recipients per Period" and "Recipients per Message".
813612	PKI authentication with customized webmail login page not working.
809363	Exporting the contact group to a .csv file exports all the address book contacts.

Common Vulnerabilities and Exposures

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

Bug ID	Description
790809	CWE-352: Cross-Site Request Forgery (CSRF)
771106	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
686309	CWE-329: Not Using a Random IV with CBC Mode
776309	CWE-121: Stack-based Buffer Overflow

Known Issues

The following table lists some minor known issues.

Bug ID	Description
594547	Due to more confining security restrictions imposed by the iOS system, email attachments included in IBE PUSH notification messages can no longer be opened properly on iOS devices running version 10 and up. Therefore, users cannot view the encrypted email messages on these iOS devices. Users should download and open the attachments on their PCs as a workaround. This issue has been resolved in FortiMail v7.0.0 release.