



FortiMail - Release Notes

Version 6.4.4

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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

February 5, 2021

FortiMail 6.4.4 Release Notes

06-644-691872-20210205

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported platforms	5
What's New	6
Special Notices	7
TFTP firmware install	7
Monitor settings for the web UI	7
SSH connection	7
Product Integration and Support	8
FortiSandbox support	8
AV Engine	8
Recommended browsers	8
Firmware Upgrade and Downgrade	9
Upgrade path	9
Firmware downgrade	9
Resolved Issues	10
Antispam/Antivirus	10
System	10
Mail delivery	11
Common vulnerabilities and exposures	11
Known Issues	12

Change Log

Date	Change Description
2021-02-04	Initial release.
2021-07-06	Added a note to Upgrade Path.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.4.4 release, build 446.

Supported platforms

FortiMail	60D, 200E, 200F, 400E, 400F, 900F, 1000D, 2000E, 3000E, 3200E
FortiMail VM	<ul style="list-style-type: none">• 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 and On-Demand• Azure BYOL and On-Demand• Google Cloud Platform BYOL

What's New

The following table summarizes the new features and enhancements in this release.

Feature	Description
MSSP: LDAP routing and recipient verification enhancement	Support LDAP routing and recipient verification when using Domain Check under System > Mail Setting > Mail Server Setting.
Option to select subject tag location	Choose where to insert the subject tag under Security > Other > Preference or by using the following CLI command: <pre>config mailsetting preference set subject-tag-location {beginning end} end</pre>

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 6.00159

Recommended browsers

For desktop computers:

- Microsoft Edge 87
- Firefox 84
- Safari 14
- Chrome 88

For mobile devices:

- Official Safari browser for iOS 14
- Official Google Chrome browser for Android 10, 11

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) > **6.4.4** (build 446)



When upgrading from 6.2.x to this 6.4.4 release, you must upgrade from 6.2.6 and older releases, not from 6.2.7 and newer 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 6.4.4 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 inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Antispam/Antivirus

Bug ID	Description
686269	Files cannot be uploaded to FortiSanbox Cloud for inspection and all the files are incorrectly displayed with the same file size.
673226	DMARC checking fails for most email from a specific domain.
684937	URL rewriting does not work properly when the original URL ends with a dot.
683293	Content filter cannot detect *.hta files for certain types of email.
660873	Impersonation analysis false positives when Header From has @ sign in the display name.
677857	DLP fingerprints fail to detect .doc files that are manually uploaded.
675212	Password protected and compressed malware files are not detected.
681435	When "Detect on failure to decompress" is enabled in the content profile, the .zip files may cause false positives.
691329	Policy match issue with LDAP verified domains.
694038	Unable to delete dynamic impersonation database entries with special characters in the Display Name.

System

Bug ID	Description
688015	Cloning a used mail routing profile, when the max entries are reached, deletes the original profile.
688008	DKIM and S/MIME signing in combination does not work properly.
682822	Some GUI items are not translated into Spanish and Portuguese.
683893	Oversized email meta data is sent to FortiSandbox.
675831	The maifilterd process causes high CPU usage.
684622	In the antispam and content action profiles, the header insertion value cannot exceed 66 characters.

Bug ID	Description
672299	In some cases, the dnscached process may get corrupted.
630571	In some cases, after a secondary unit reboots in a config only HA, it cannot resynchronize with the primary unit
674038	When the registration expiry time under IBE Encryption setting is set to 0, the registration/reset link should never expire.
681338	FortiMail server mode calendar subscription on Outlook using the iCal URL is not working.
679151	A Gmail account using a "+" plus symbol for an alias will cause issues with IBE account creation on FortiMail.
681775	Incorrect subject encoding modifies cross search log lines.
691523	Unexpected quotation marks in blocklists when exporting the configuration.
691596	In FIPS-CC mode, FortiMail fails to import a local certificate due to the lack of certificate CRL.
691549	After adding a new webmail custom language under System > Customization > Appearance, the IBE registration web portal stops working.
693194	When hide-on-email-arrival is enabled with Microsoft 365 real-time scanning, duplicate folders may be created in the mail user inbox.

Mail delivery

Bug ID	Description
673911	Webmail client IP address is used in EHLO when sending DSNs for IBE reply email.

Common vulnerabilities and exposures

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

Bug ID	Description
690894	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').
692223	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').
693465	CWE-36: Absolute Path Traversal.
694366	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Known Issues

The following table lists some minor known issues.

Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
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.



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.