



FortiMail - Release Notes

Version 6.4.5



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://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

June 10, 2021

FortiMail 6.4.5 Release Notes

06-645-724152-20210610

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
System	9
Log and Report	10
Common vulnerabilities and exposures	10
Known Issues	12

Change Log

Date	Change Description
2021-06-10	Initial release.
2021-06-30	Added a note to Upgrade Path.

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 6.4.5 release, build 453.

Supported models

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

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 6.2.162

Recommended browsers

For desktop computers:

- Microsoft Edge 88
- Firefox 89
- Safari 14
- Chrome 91

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) > **6.4.5** (build 453)



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 6.4.5 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
700919	Issues when scanning PDF files.
714175	Content profile actions are not applied correctly for Zip archives containing an .exe file and an MS Office macro file.
707494	For some email, FortiMail may get NoResult response from FortiSandbox.
660873	Impersonation Analysis false positives.
709825	Fail to detect files with .js extension included in BZIP2 archives.
713397	DLP attachment metadata detection doesn't work for docx and xlsx files.
719997	MS365 internal email is scanned by the first enabled policy.
713859	Fail to detect macros in Excel legacy format *.xls files.
702940	Regular expressions are not detected in XLS files.
702148	Invalid top-level domain addresses are rejected in relaxed email parsing mode.
705753	Double stamping removal only works on full domains, not on subdomains.
709083	Fail to allow PDF files in some cases.
712099	Password protect .7z files are incorrectly blocked.
710968	After FortiMail/FortiSandbox processes the email, the email is moved to the user's inbox, instead of the original custom folder.

System

Bug ID	Description
679151	Gmail using a "+" plus symbol for an alias causes issues with IBE account creation.
702595	CSR download button is grayed out under System > Certificate > Local Certificate.

Bug ID	Description
716038	Expired IBE users are not displayed on the GUI.
700244	For Diffie-Hellman key exchange, FortiMail uses self-generated parameters, which are different from the predefined finite field groups in RFC 7919 .
691596	In FIPS-CC mode, importing a certificate via the GUI fails with the message "Unable to get certificate CRL."
608247	LDAP authentication does not work for newly created domains.
707925	RADIUS 2FA users are locked out after the first unsuccessful login attempt.
699918	IBE customized template for 2FA secure token notification is not taking the changes on the "From" field.
693981	Fail to connect to the SMB/CIFS server under Data Loss Prevention > Sensitive Data > FingerPrint Source.
712577	High CPU usage when scanning PDF files.
705376	After upgrading, the customized IBE language is lost.
692164	Possible to create identical greylist exempt entries.
720374	When importing mail users from .csv files, the users cannot log in.
719654	No system event logs for changes (add/delete) in user secondary accounts.
720910	LDAP routing and recipient verification are not working as expected in 6.4.4 release.

Log and Report

Bug ID	Description
681775	Incorrect email subject encoding modifies the cross search log lines.
721435	Problem with log display and overwriting.
707915	When certain zip files are decrypted, the action is not logged.

Common vulnerabilities and exposures

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

Bug ID	Description
691547 692463	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').
697251	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Bug ID	Description
693465	CWE-36: Absolute Path Traversal.
694366	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').
694751	CWE-310: Cryptographic Issues.
695037 694752	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').
695039	CWE-131: Incorrect Calculation of Buffer Size.
700994 700991	CWE-401: Missing Release of Memory after Effective Lifetime.
698764	CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG).
696793	CWE-325: Missing Cryptographic Step.

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.



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.