FortiMail - Release Notes

Version 6.4.3

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

October 16, 2020
FortiMail 6.4.3 Release Notes
06-642-670585-20201016

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-10-16	Initial release.
2021-06-25	Added one item to What's Changed section.
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 6.4.3 release, build 437.

Supported platforms

FortiMail	60D, 200E, 200F, 400E, 400F, 900F, 1000D, 2000E, 3000E, 3200E
FortiMail VM	• VMware vSphere Hypervisor ESX/ESXi 5.0 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
Support grep utility in CLI	Support pipe grep in CLI, including show, get, and diagnose commands.
Disclaimer in email replies	New CLI command to enforce disclaimers in email replies (under `config mailsetting preference`).
Option to disable CDR disclaimer	New CLI command to enabe/disable CDR disclaimer (`under config file content-disarm-reconstruct`).
FortiSandbox Cloud enhanced service	In addition to the shared FortiSandbox Cloud service, support for an enhanced dedicated Cloud service has been added. For details, see the FortiMail Administration Guide or online help.
Log message viewing navigation	Added Previous and Next buttons in the log message popup window to facilitate log message viewing navigation.
HA terminology	Renamed HA terms. Now using Primary and Secondary.

What's Changed

The following table summarizes the behavior changes in this release.

Feature	Description
FortiGuard antispam actions	When FortiGuard detects spam for both IP reputation and URL category in an email, the URL category action will be taken and logged. For example, if the IP reputation action is "Tag" while the URL category action is "Reject", the email will be rejected. Before v6.4.3, the IP Reputation action will be taken and logged instead.

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 6.00153

Recommended browsers

For desktop computers:

- Microsoft Edge 85
- Firefox 81
- Safari 14
- Chrome 85

For mobile devices:

- Official Safari browser for iOS 13
- Official Google Chrome browser for Android 9, 10

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)> **6.4.3** (build 437)

When upgrading from 6.2.x to this 6.4.3 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 6.4.3 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
669438	Email classified as "TLS Session" shouldn't be counted as spam in spam reports.
667425	DOCX files uploaded into DLP sensitive data fingerprint are not detected.
666868	ISO attachments are not detected by file MIME type.
663105	Microsoft 365 real-time protection cannot move back hidden-on-arrival email to non-English named inboxes.
662953	Invalid URLs in email may cause email rejection.
663091	When recipient verification is enabled, and after enabling Automatic Removal of Invalid Quarantine Accounts (SMTP), recipient verification is set back to none.
624567	URI click protection does now work properly in some cases.

System

Bug ID	Description
669983	In some cases, recipient verification over SMTPS may cause high CPU usage.
669717	Customized settings in notification templates are not applied in Microsoft 365 profiles.
669152	Administrator idle timeout does not work for REST API login.
666027	Microsoft 365 threat remediation connection fails due to SSL certificate issue (unable to get local issuer certificate).
663093	Issue with IBE token verification setting for mobile numbers from Norway.
663290	When email address parsing mode is set to relaxed, gateway mode also loosens LDAP recipient verification and allows non-existing hosts.
669689	No DSNs are sent after the email in queue reaches the maximum time.
667723	Administrators with read-only admin profiles to "Others" can modify IBE settings.

Mail delivery

Bug ID	Description
663329	In some cases, FortiMail transparent mode intermittently stops passing traffic.

Webmail

Bug ID	Description
662754	When sending an encrypted email, image files may not be attached in some cases.

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.