FortiMail - Release Notes

Version 6.4.2

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

September 23, 2020
FortiMail 6.4.2 Release Notes
06-642-658582-20200923

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-09-02	Initial release.
2020-09-23	Added TLS recipient verification in What's New section.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.4.2 release, build 427.

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 0.12.1 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
Apply button confirmation	After the Apply button is clicked on the GUI, a confirmation message "Changes have been saved." will be displayed.
DLP fingerprint generation indicators	When fingerprints are generated under Data Loss Prevention > Sensitive Data > Fingerprint, the generation status will be displayed.
MS365 notification information	MS365 notification count and delay information will be displayed on the dashboard and FortiView.
IBE account validation before registration	When enabled, IBE users will receive a validation email that contains an activation link to complete account registration.
DMARC policy enhancement	New CLI command to handle "p=none" record.
Recipient verification TLS support	New CLI command to enable TLS if the backend server enforces TLS connection.

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 44, 84
- Firefox 80
- Safari 13
- 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)> **6.4.2** (build 427)

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 6.4.2 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
652437	Email body may not show in Microsoft Outlook when URL click protection is enabled.
652415	Content scanning handles .xls and .xlsm files improperly.

System

Bug ID	Description
655958	When the remote archive server is not reachable, the mail queue may cause high disk usage.
651652	Envelope From is missing in IBE two factor authentication notification email.
656401	IP pools disappear from the access control delivery policies on HA config slave units after certain configuration changes.
654451	In some cases, mailfilterd may cause high CPU usage.
652067	After upgrading from 6.2 to 6.4 release, the Recipient To parameter is changed in the quarantine report.

Admin GUI and webmail

Bug ID	Description
653435	The error message displayed when resetting the IBE password is incorrect.

CLI

Bug ID	Description
653179	"execute erase-filesystem" command returns wrong partition size information.

Common vulnerabilites and exposures

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

Bug ID	Description
648817	FortiMail 6.4.2 is no longer vulnerable to the following CVE-Reference: • CVE-2020-15933

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.