



FortiMail - Release Notes

Version 6.2.2

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



November 28, 2019

FortiMail 6.2.2 Release Notes

06-622-000000-20191128

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
Recommended browsers on desktop computers for administration and webmail access	7
Recommended browsers for mobile devices for webmail access	7
FortiSandbox support	7
SSH connection	8
Firmware upgrade and downgrade	9
Upgrade path	9
Firmware downgrade	9
Resolved issues	10
Profiles	10
Mail receival and delivery	10
System	10
Known issues	12

Change Log

Date	Change Description
2019-11-28	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.2.2 release, build 263.

Supported platforms

- FortiMail 60D
- FortiMail 200E
- FortiMail 200F
- FortiMail 400E
- FortiMail 400F
- FortiMail 900F
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2, 2016)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher)
- FortiMail VM (AWS BYOL and On-Demand)
- FortiMail VM (Azure BYOL and On-Demand)

What's new

There are no new features introduced in this patch release.

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.

Recommended browsers on desktop computers for administration and webmail access

- Internet Explorer 11 and Edge 42, 44
- Firefox 60.8 ESR, 68
- Safari 12
- Chrome 75

Recommended browsers for mobile devices for webmail access

- Official Safari browser for iOS 11, 12
- Official Google Chrome browser for Android 7.0 to 9.0

FortiSandbox support

- FortiSandbox 2.3 and above

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.

Firmware upgrade and downgrade

Before any firmware upgrade or downgrade, save a copy of your FortiMail configuration by going to **Dashboard** > **Status** and click **Restore** 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) > **6.2.2** (build 263)

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 6.2.2 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 inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Profiles

Bug ID	Description
589530	When malware/virus outbreak protection is enabled, URIs will not be submitted to FortiSandbox for scanning.
590888	In some cases, FortiMail fails to parse URLs in email body and send them to FortiSanbox inspection.
591868	In DLP rules, the scan condition "Recipient is internal" does not work.
593942	When URLs miss the second slash, that is, http:/ instead of http://, URI scan cannot be handled properly.
595120	In some cases, email messages may stay in the FortiSandbox mail queue for too long and cause delivery delays.
595592	After upgrading to 6.2.0 or 6.2.1 releases, spam email cannot be detected by Heuristic rules anymore.
596913	Regular expression does not work in between ^ and \$ signs.

Mail receipt and delivery

Bug ID	Description
589835	Enabling header manipulation without any configured headers to remove may cause mail relay issues.
589578	When using the IBE pull method, email message formats may be distorted in Microsoft clients.
594142	After upgrading to 6.2.1 release, mailfilterd may stop working for some malformed attachments.

System

Bug ID	Description
592401	FortiMail CardDAV URL does not work with eM Client.
588576	Spam reports display the Header From as UTF-8 encoded values, instead of email addresses.

Bug ID	Description
593841	High memory usage of Idapcached.
595080	LDAP user settings cannot be preserved after editing the user password.

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.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.
(No bug ID)	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.



FORTINET[®]



Copyright© 2020 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.