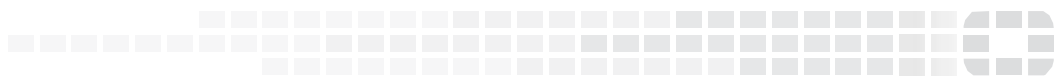




FORTINET
High Performance Network Security



FortiMail™ Release Notes

VERSION 5.3.7 GA



FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



October 25, 2016

FortiMail™ 5.3.7 GA Release Notes

TABLE OF CONTENTS

Introduction	4
Supported Platforms	4
What's New	5
What's Changed	6
Special Notices	7
TFTP firmware install	7
Monitor settings for web UI	7
Recommended browsers on desktop computers for administration and Webmail	7
Recommended browsers on mobile devices for Webmail access	7
FortiSandbox support	7
Firmware Upgrade/Downgrade	8
Before and after any firmware upgrade/downgrade	8
Upgrade path	8
For any 5.x release	8
For any 4.x release	8
Firmware downgrade	9
Downgrading from 5.3.x to 5.x or 4.x releases	9
Resolved issues	10
MTA/Proxy	10
System	10
Log and Report	10
Image checksums	11

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiMail™ Release 5.3.7, build 0623.

Supported Platforms

FortiMail 5.3.7 release supports the following platforms:

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400C
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000B
- FortiMail 2000E
- FortiMail 3000C
- FortiMail 3000D
- FortiMail 3000E
- FortiMail 3200E
- FortiMail 5002B
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FortiMail VM [AWS(BYOL)]
- FortiMail VM [Azure(BYOL)]

What's New

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

Features	Descriptions
IBE sub folders	On the IBE webmail GUI, users can now create sub folders for the IBE messages and manually move messages among all IBE folders.

What's Changed

The following table summarizes the changes to the functionalities, GUI, and CLI.

Features	Descriptions
FortiCloud Service	<p>The FortiMail Cloud submission limits introduced in FortiMail 5.3.5 have been removed and are no longer enforced in FortiMail 5.3.7.</p> <p>If submitting large volume of files to FortiSandbox Cloud, you may experience situations where response timeouts occur. To modify the scan timeout, go to AntiVirus > FortiSandbox. .</p>

Special Notices

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 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

- Internet Explorer 11 and Edge 20, 25, 38
- Firefox 40 to 49
- Safari 8 to 10
- Chrome 45 to 53
- Adobe Flash Player 9 or higher plug-in required to display statistics charts

Recommended browsers on mobile devices for Webmail access

- Official Safari browser for iOS 8 to 10
- Official Google Chrome browser for Android 5.0 to 7.0

FortiSandbox support

The current FortiMail release requires FortiSandbox 2.1 or newer releases. FortiSandbox 2.3 or new releases are highly recommended.

Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *Maintenance > System > Configuration*.
- After any firmware upgrade/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.
 - 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.

Upgrade path

For any 5.x release

Any 5.x release older than 5.2.6

-

5.2.6 (Build 460)

-

5.2.8 (Build 467)

-

5.3.7 (Build 623)

For any 4.x release

Any 4.x release older than 4.3.6

-

4.3.6 (Build 540)

-

5.2.6 (Build 460)

-

5.2.8 (Build 467)

-

5.3.7 (Build 623)

After every upgrade, verify that the build number and branch point match the image that was loaded by going to *Monitor > System Status > Status* on the Web UI.

Firmware downgrade

Downgrading from 5.3.x to 5.x or 4.x releases

Downgrading from 5.3.x release to any 5.x or 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 5.3.x 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 5.3.x 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](#).

MTA/Proxy

Bug ID	Description
391183	In transparent mode, FortiMail sends the DSN messages to the DSN sender rather than the protected domain's configured email server.

System

Bug ID	Description
391025	End of Daylight Savings (DST) in Turkey/Istanbul time zone.
392409	When an admin profile is renamed, the SSH key get lost.
391638	After system reboot, the "session-profile-rate-control-interval" returns to the default value.

Log and Report

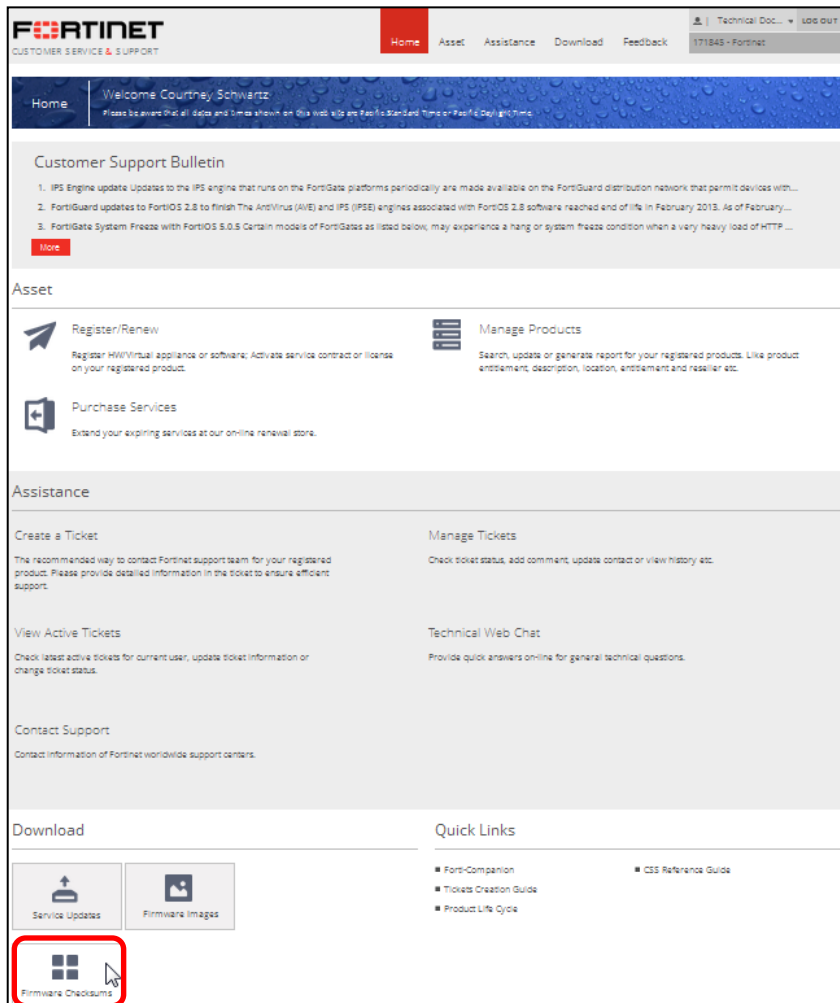
Bug ID	Description
392072	If a policy is configured to monitor but not to prevent spam, the history logs will display "Not Spam" classifier for spam messages.
392034	Remote logging should not stop after FortiMail system reboot

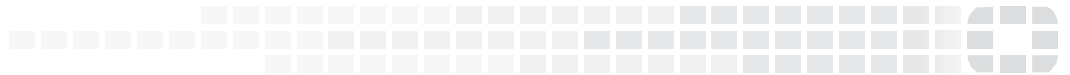
Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool





Copyright© 2016 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.