FortiMail™ Release Notes

VERSION 5.0.10 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

April 29, 2016

FortiMail™ 5.0.10 GA Release Notes

TABLE OF CONTENTS

Introduction 4
Supported Platforms 4
Special Notices 5
TFTP firmware install 5
Monitor settings for web UI 5
Recommended web browsers 5
Firmware Upgrade/Downgrade 6
Before and after any firmware upgrade/downgrade 6
Upgrade path 6
For any 5.x release 6
For any older 4.x release 6
Firmware downgrade 7
Resolved issues 8
Antispam/Antivirus 8
MTA/Proxy 8
System 8
Image checksums 9

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiMail™ Release 5.0.10, build 0186.

Supported Platforms

This FortiMail release supports the following platforms:

- FortiMail 100C
- FortiMail 200D
- FortiMail 400B
- FortiMail 400C
- FortiMail 1000D
- FortiMail 2000B
- FortiMail 3000C
- FortiMail 3000D
- FortiMail 5001A
- FortiMail 5002B
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)

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 web browsers

- Internet Explorer 11
- Firefox 24 to 31
- Safari 5 to 8
- Chrome 23 to 39
- Adobe Flash Player 9 or higher plug-in required to display statistics charts

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 5.0.x GA release

–

5.0.10 (Build 186)

For any older 4.x release

Any 4.x release older than 4.3.6

–

4.3.6 (Build 540)

–

5.0.10 (Build 186)

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 5.0.x release to and 5.x and 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 5.0.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 5.0.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 inquires about a particular bug, please contact Fortinet Customer Service & Support.

Antispam/Antivirus

Bug ID	Description
368516	Address mapping rules are not applied to email released from system quarantine.
368679	Japanese characters are garbled if the "Remove hidden HTML content" option is enabled in the content profile.
365161	Quarantine reports are not sent out with FortiMail VM gateway mode for Microsoft Hyper-V Server.

MTA/Proxy

Bug ID	Description
355519	Reverse DNS pattern does not work if the client IP is forged.

System

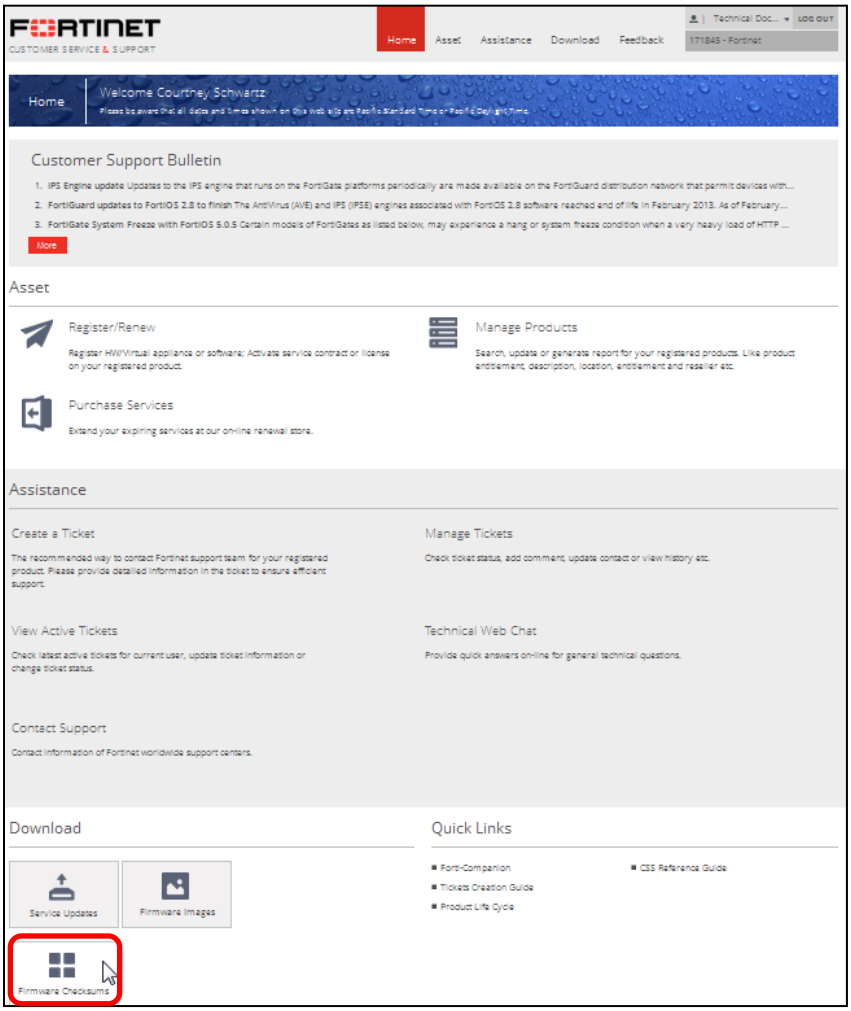
Bug ID	Description
356715	OpenSSL Security Advisory [1 March 2016]
307928	OpenSSL Advisory 28th January 2016

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© 2015 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.