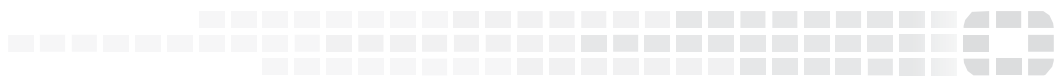




FORTINET

High Performance Network Security



FortiMail™ Release Notes

VERSION 6.0.2 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



August 9, 2018

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 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
SSH connection.....	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 6.0.2 to 5.x or 4.x releases.....	9
Resolved Issues	10
Antispam/Antivirus/Content	10
System	10
Log and Report.....	10
Admin GUI/Webmail	10
Known Issues	11
Image Checksums	12

Change Log

Date	Change Description
2018-08-02	Initial release.
2018-08-09	Added Microsoft Hyper-V Server 2016 and Open Source XenServer as supported platforms.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.2 release, build 0108.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000D
- 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)]
- FortiMail VM [Azure(BYOL)]

What's New

There are no new features in this patch release.

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 40, 41
- Firefox 52.7.2 ESR, 59
- Safari 10, 11
- Chrome 65

Recommended browsers on mobile devices for Webmail access

- Official Safari browser for iOS 10, 11
- Official Google Chrome browser for Android 6.0 to 8.0

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.

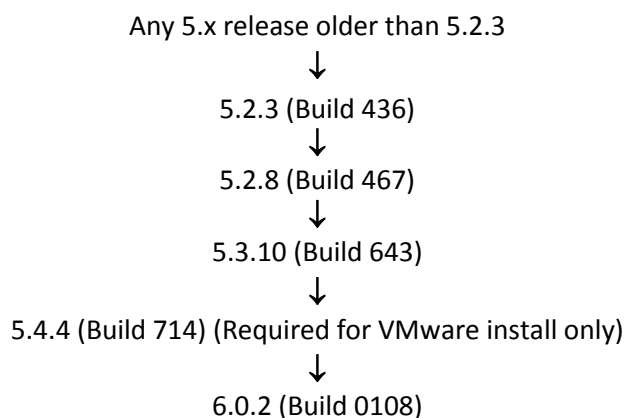
Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

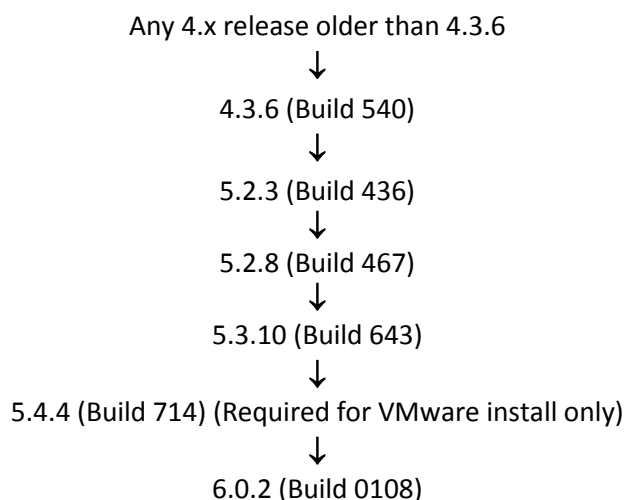
- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *System > Maintenance > Configuration*.
- After any firmware upgrade/downgrade:
 - If you are using the web UI, clear the browser cache prior to login on the FortiMail unit 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



For any 4.x release



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

Firmware downgrade

Downgrading from 6.0.2 to 5.x or 4.x releases

Downgrading from 6.0.2 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 6.0.2 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](#).

Antispam/Antivirus/Content

Bug ID	Description
502254	File filters with "Is Not" operator are still detected by content profiles based on the file type.
486092	FortiGuard web service might incorrectly identify some URI as "Newly Observed Domain".
447735	Part of email body is lost after converting from HTML to text.
504494	When URI Selection is set to "None" under System > FortiSandbox, FortiMail will not send files to FortiSandbox.

System

Bug ID	Description
503047	Not able to mount SMB/CIFS shares.
498777	It is not possible to map to multiple contact fields while doing LDAP address book import (server mode only).
503980	When the system is changed from none FIPS mode to FIPS mode or vice versa, login will fail.
502966	When importing a certificate, a password is always required even though the certificate does not have a password.
502549	Calendar entries are deleted when connection to NAS storage is lost.

Log and Report

Bug ID	Description
502410	No logs when the operation mode is changed manually.
502037	Changes to safe/block lists are not logged.
502563	When any user edits the SNMP configurations, the system logs always show the user as "admin".

Admin GUI/Webmail

Bug ID	Description
503141	Viewing or releasing system quarantined email from the history log right-click menu is not successful in some cases.
500180	Folder names are not displayed properly when the webmail GUI is set to certain languages.

Known Issues

The following table lists some minor known issues. .

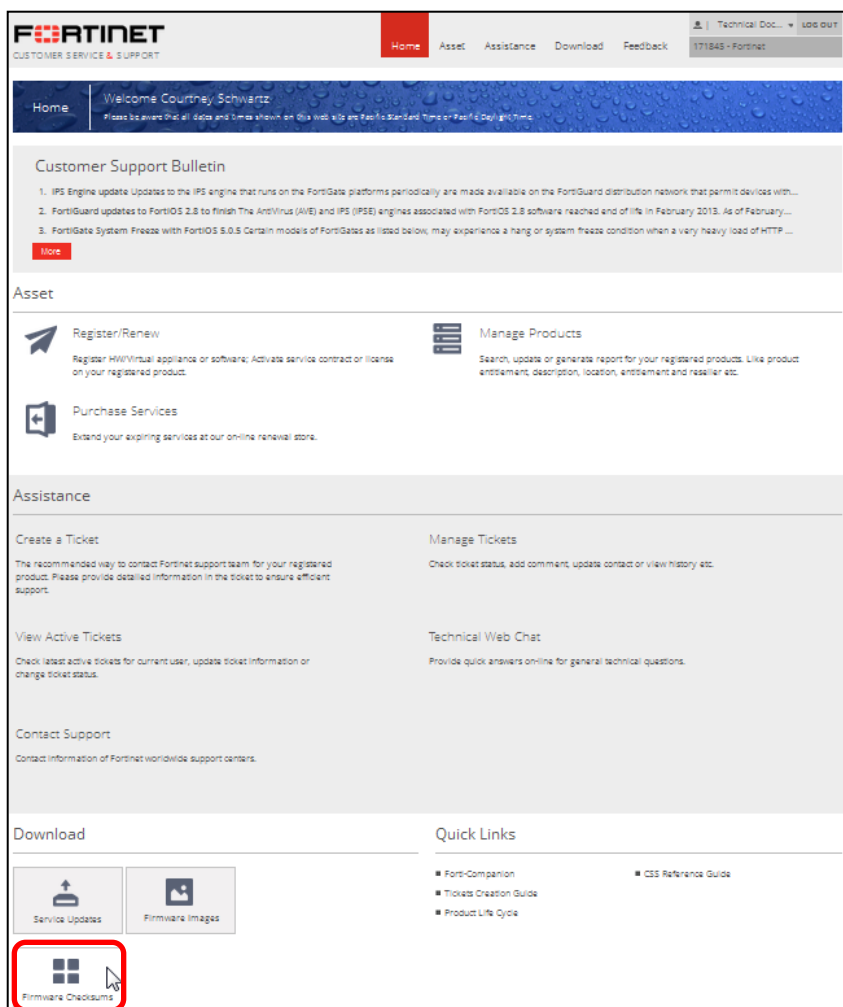
Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

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



FORTINET

High Performance Network Security



Copyright© 2018 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.