FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 6.0.6 GA

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 COOKBOOK

https://cookbook.fortinet.com

FORTINET TRAINING SERVICES

https://www.fortinet.com/training

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 25, 2019

TABLE OF CONTENTS

Change Log 4
Introduction 5
  Supported Platforms 5
What's New 6
What's Changed 7
Special Notices 8
  TFTP firmware install 8
  Monitor settings for web UI 8
  Recommended browsers on desktop computers for administration and Webmail 8
  Recommended browsers on mobile devices for Webmail access 8
  FortiSandbox support 8
  SSH connection 8
Firmware Upgrade/Downgrade 9
  Before and after any firmware upgrade/downgrade 9
  Upgrade path 9
  Firmware downgrade 10
    Downgrading from 6.0.6 to 5.x or 4.x releases 10
Resolved Issues 11
  Antispam/Antivirus/Content/Session 11
  Mail Receiving/Delivery 11
  System 11
  Admin GUI/Webmail 12
  Common Vulnerabilities and Exposures 12
Known Issues 13
Image Checksums 14

Change Log

Date	Change Description
2019-07-25	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.6 release, build 0156.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 200F
- FortiMail 400E
- FortiMail 400F
- FortiMail 900F
- 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 and On-Demand)
- FortiMail VM (Azure BYOL and On-Demand)

What's New

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

Features	Descriptions
LDAP group expansion	Added group level expansion to LDAP profile configuration. For details, see the FortiMail Administration Guide.
New variable in quarantine reports	The envelope MAIL FROM address can now be added as a variable in the quarantine report template.

What's Changed

The following table summarizes the behavior changes in this release.

Features	Descriptions
FIPS-CC mode enabling	Removed the ability to enable FIPS-CC mode from SSH. It can only be done via the console now.
Password policy in FIPS mode	In FIPS mode, empty admin passwords are not allowed and the password policy will be followed as well.
IA scan	In addition to the Header From field, Impersonation Analysis also inspects the Reply-To field now.
IA bypass	Impersonation Analysis will not be bypassed for ACL rule matches.
Quarantine report variable	The variable %%MESSAGE_ID%% is renamed to %%EMAIL_ID%% to avoid confusion. The email ID is assigned by FortiMail to the quarantined email while the message ID is the standard message ID in the email header.
DKIM signing	Header From domain is used for DKIM signature now. Envelope From domain was used before.
Archive account storage quota	Instead of capping disk space for an individual account as 20% of the mail partition on the remote storage, disk usage for all the archive accounts will be capped to 80% now.

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 42, 44
- Firefox 60.8 ESR, 68
- Safari 12
- Chrome 75

Recommended browsers on 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/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

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)

↓

6.0.6 (Build 156)

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 6.0.6 to 5.x or 4.x releases

Downgrading from 6.0.6 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 6.0.6 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/Content/Session

Bug ID	Description
569960	DLP with profanity setting does not work.
557805	Regular expressions in DLP rules and content monitor do not match contents in HTML links.
567801	For URI protection scan, FortiMail and FortiSandbox Cloud have communication issues.
568910	BCC action in the content profile does not work if DSN email generation is disabled.
567511	Rewrite From in the session profile does not work if Header From is missing.
563130	In some cases, header manipulation may not work properly.
569416	Impersonation Analysis should not be bypassed for ACL rule match.
568281	Impersonation Analysis is bypassed when an email message contains multiple recipients.
573097	When using a customized file filter in a content profile, the .pub files are caught by the MS PowerPoint filter, instead of the MS Publisher filter.

Mail Receiving/Delivery

Bug ID	Description
553478	In some cases, received email is not delivered.
556364	Recipient Address Verification does not work when the internal mail server responds to SMTP connections with warning messages.
565422	SMTP connections timeout on incoming mail. FortiMail should send EOM responses after receiving all data.
530592	When both URI Click Protection and MS Office/PDF CDR are enabled, there will be milter exception error.

System

Bug ID	Description
561924	Nested LDAP groups deeper than two levels cannot be found.
572514	Error message when resetting an IBE user.
565860	After system reboot, IP pools fail to answer SMTP connections.
498174	LDAP alias expansion should not be case sensitive.

Bug ID	Description
551045	In some cases, mailfiltered may cause high CPU usage on HA pairs.
514185	Under certain conditions, Cyrillic alphabets from some domains show incorrect encoding.
558429	Config-only HA members should not have the same entity IDs.
554636	FortiMail can be accessed from any IP address even if the IP address is different from the trusted host.

Admin GUI/Webmail

Bug ID	Description
563496	Multiple attachments cannot be uploaded and sent properly in webmail.
565536	Under Security > Quarantine > Quarantine Report > Web release host name/IP, a port number cannot be added.
556550	Some columns of the policy table are not displayed properly.
560618	The system quarantine folder cannot be opened when the folder name contains Japanese characters.
564553	In some cases, the FotiSandbox statistics are not displayed properly under *FortiView* > *Threat Statistics* > *FortiSandbox Statistics*.
554898	Expired administrators are still displayed in the current administrator list if the administrators closed the browser without logging out from the admin GUI.

Common Vulnerabilities and Exposures

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

Bug ID	Description
565946	FortiMail 6.0.6 is no longer vulnerable to the following CVE-Reference: • CVE-2019-11478 • CVE-2019-11479
565904	FortiMail 6.0.6 is no longer vulnerable to the following CVE-Reference: • CVE-2019-11477
568641	FortiMail 6.0.6 is no longer vulnerable to the following CVE-Reference: • CVE-2019-0217
569759	FortiMail 6.0.6 is no longer vulnerable to the following CVE-Reference: CVE-2019-12900

Known Issues

The following table lists some minor known issues. .

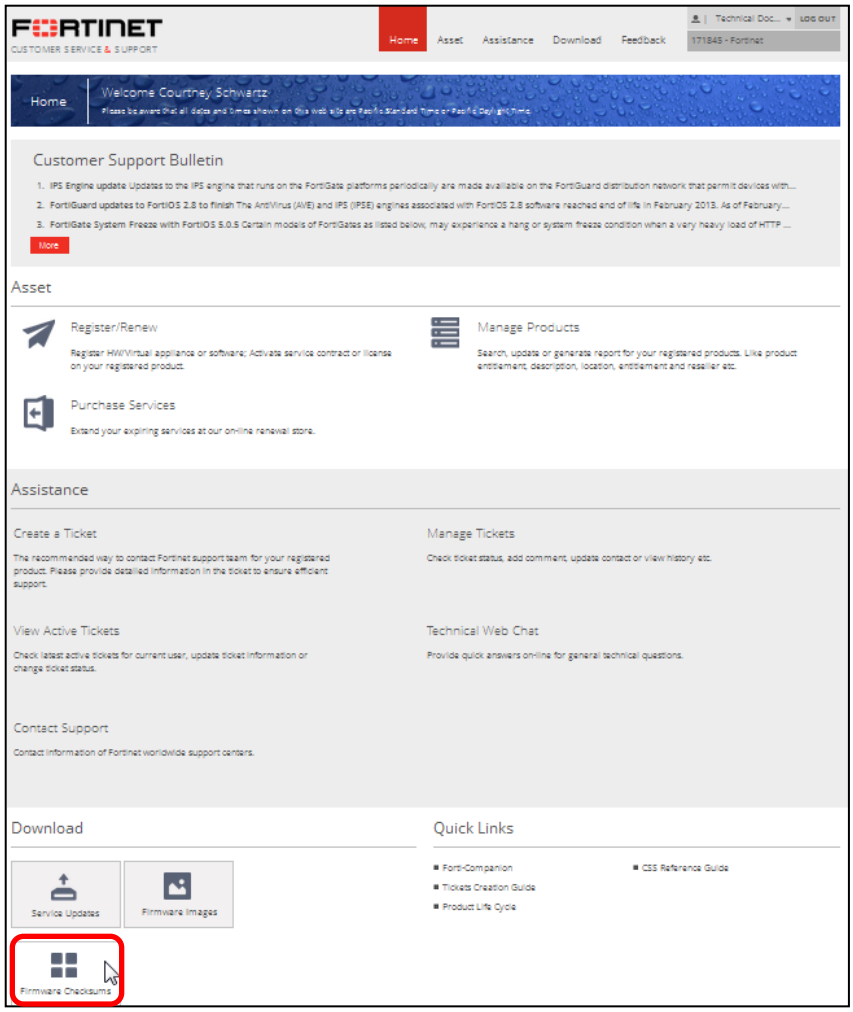
Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

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



Copyright© 2019 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.