FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 6.0.4 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

February 13, 2019

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-02-13	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.4 release, build 0143.

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
Original URI in URI click protection (Mantis bug 524328)	The rewritten URI format will include information of the original URI, which can be decoded to get the original URI.

Loose RFC compliance check option (Mantis bug 521283)	The following CLI command has been added to allow non-RFC compliant local part in the sender and recipient addresses. The default is strict. For details, see the FortiMail CLI Reference.
	`config mailsetting email-addr-handling`
	`  set email-addr-parsing-mode {strict | relaxed}`
	`end`

FortiGuard URI aggressive checking	From 6.0.4 release, the aggressive setting of FortiGuard URI filter and scanning start to scan the domain part of envelope MAIL FROM, header From, and Reply-To addresses. If the domains are identified as spam, the configured antispam actions will be applied.
New LDAP filter variable (Mantis bug 533568)	A new filter $f has been added. It expects the attribute's value to be a sender domain name. $S has been changed to $s.

What's Changed

The following table summarizes the behavior changes in this release.

Features	Descriptions
Administrator privileges	Starting from this release, administrators with Read Only privileges to System Quarantine, Personal Quarantine, Archive, and Mail Queque categories cannot view emal contents anymore. Only administrators with Read-Write privileges can view email contents.
Impersonation check	The old behavior can bypass impersonation check if the sender is exempted in the greylist. The new behavior still performs impersonation check even if the sender is exempted in the greylist.
LDAP query maximum timeout	Increase LDAP query maximum timeout value from 60 to 120 seconds.
Attempt to decrypt in content profile	“Attempt to decrypt archive” no longer requires to enable “Detect password protected archive” first. This means that if the decryption action fails, the message will be passed.
Only greylist new MTAs	Only greylist email messages that originate from new MTAs.

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 60.5 ESR, 65
- Safari 11, 12
- Chrome 71

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)

↓

6.0.4 (Build 143)

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 6.0.4 to 5.x or 4.x releases

Downgrading from 6.0.4 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 6.0.4 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

Bug ID	Description
536232	Session Settings action discards email when set to personal quarantine.
532266	DKIM signatures should not be added to email with empty header From.
529854	When sender rate control is triggered by virus, the notification email is empty.
521652	Scan order issue with ISO files.
531333	Unable to decompress certain tar files.
530592	In some cases, content monitoring may cause MilterException errors.
524848	Notification email contains empty variables for file names and file types.
522821	All rich text email messages are sanitized by CDR (content disarm and reconstruction).
521347	URI click protection may get timeout or wrong verdict from FortiSandbox.
528389	In some cases, spam email may cause error messages.
518789	Invisible characters may cause dictionary and banned word scan to fail.

Mail Receiving/Delivery

Bug ID	Description
531152	FortiMail drops connections for email that contains specially formatted HTML parts.
512906	In gateway mode, it takes 5-10 seconds to send 220 responses for SMTP requests from specific SMTP clients.
526680	After upgrading to 6.0.3 release, email messages sent from certain MTAs may get dropped.
529686	Mailfilterd will exit unexpectedly when doing CDR (content disarm and reconstruction) scan for certain email messages.
527130	A distribution list can only be expanded to a maximum of 1500 recipients.
531332	Email may not be delivered in some circumstances if URI Click Protection is enabled in the Content Profile.

Common Vulnerabilities and Exposures

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

Bug ID	Description
524928	FortiMail 6.0.4 release is no longer vulnerable to the following CVE Reference: • CVE-2018-5407

System

Bug ID	Description
522006	WCCP between FortiGate and FortiMail does not work.
531012	Unable to retrieve FortiSandbox verdict for some URIs.
530674	In HA mode, when the master cannot access the read only filesystem, it should fail over to the slave.
529670	IP pools are not working after upgrading from 5.4.3 to 6.0.3 release.
531574	Intermittent issues with DNS and recipient verification.
519213	In some cases, the slave units in a Config HA cluster will remain in out-of-sync state.
528291	Changing the FortiMail operation mode on Azure resets the settings and the administrator cannot log in back to the instance anymore.
524885	FortiMail should not send queries of its own hostname to the DNS server.
527573	In some cases, the httpd process stops working on the slave units in a config HA cluster.
525772	In some cases, mailfitlerd may cause high CPU usage.

Log and Report

Bug ID	Description
524671	The log file shows the attachment filter action but does not show the attachment file name.
537358	Misleading logs are generated when using LDAP profile with mail routing and address mapping with more than one internal address.

Admin GUI/Webmail

Bug ID	Description
522438	Web quarantine report link without authentication stops working after upgrading to 6.0.3 release.
529609	Japanese translation is not complete in the admin GUI.
530405	In the Quick Start Wizard, the configured time zone is displayed incorrectly in step 8.
527839	Japanese translation is wrong on System > High Availability > Status.

Bug ID	Description
524858	Configurations of smart identifiers in a dictionary profile are reset to default after the dictionary profile is modified.
525639	Some description column in the custom messages are empty.

Known Issues

The following table lists some minor known issues. .

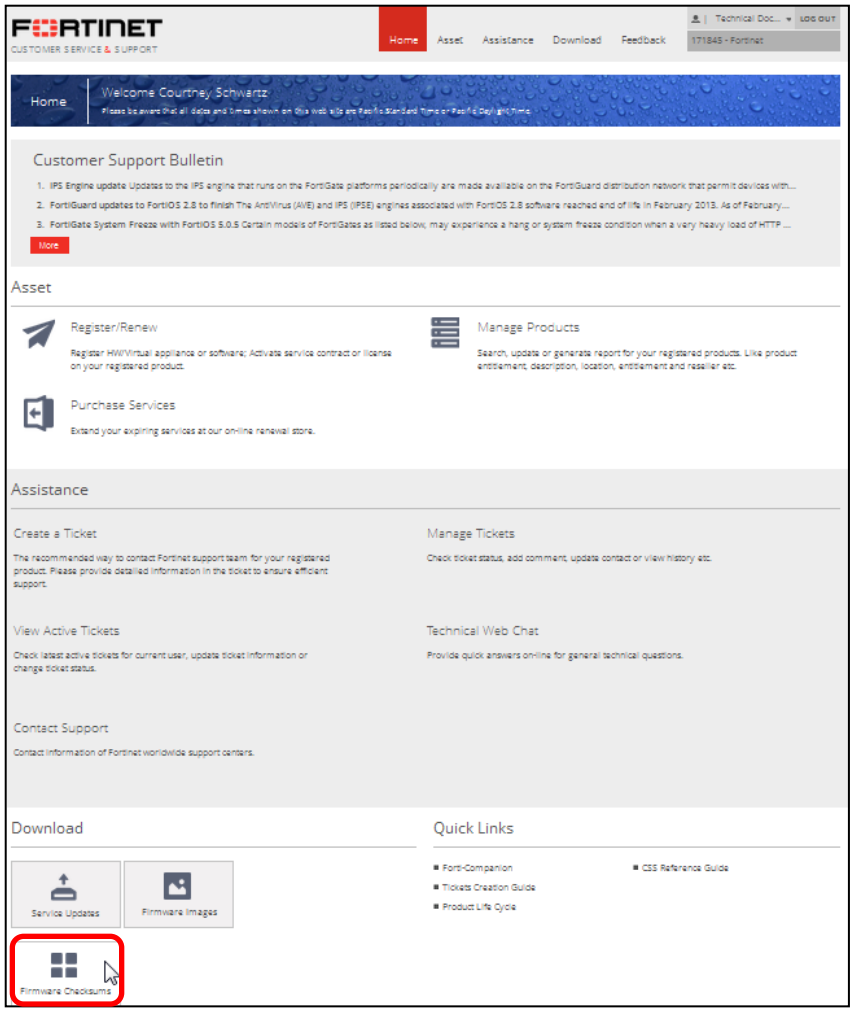
Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

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.