FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 5.4.0 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 5, 2018

TABLE OF CONTENTS

Introduction

FortiMail 5.4.0 GA build 692 is a major release. It comes with a GUI restructure and many new features and enhancements.

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

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)
- 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
FortiGuard Virus Outbreak Protection Service (license needed)	Support the service in case of virus outbreaks.
Dynamic Adult Image Analysis Service (license needed)	Detect embedded or attached adult images in email.
SAML SSO	Support SAML v2.0 Single Sign-On to FortiMail webmail.
Password decryption for archive and PDF files	Use email keywords, built-in password list, or user-defined passwords to decrypt password protected archive and PDF files.
Extreme virus database support	In addition to the regular virus and extended virus database, FortiMail 1000D/VM04 and higher platforms now support the extreme virus database, which includes viruses that are no longer seen in the wild.
MX record for associated domain	In transparent and gateway mode, when a domain association is used and the domain's relay type is set to MX record (this domain) or MX record (alternative domain), an option is added to choose between the MX record of the main domain or the associated domain.
HA synchronization	Personal safe/block lists will be synchronized in a config only HA cluster.
Undo email sending	In webmail, an option is added to allow users to delay email sending for a certain period of time, in case the users want to cancel email delivery.
Two-factor authentication for administrators	Support two-factor authentication for admin users.
DKIM signing	Use key of main domain to sign associated domains.
EGG and 7-Zip file support in content profiles	Support extracting contents in EGG and 7-Zip files.
Maximum size of email and attachments in content profiles	Support blocking email with maximum email size and/or attachment size.
SMB 2/3 support	Support SMB version 2 and 3 in Data Loss Prevention and mail data backup. Removed version 1 support.
Action on unrated URI	Different actions can be take towards unrated URIs other than the actions towards other

Features	Descriptions
	known bad URIs.
AV update trap	Added alert email and SNMP trap for FortiGuard AV update/connection failures.
PDF embedded files	Detect files embedded in PDF files.
Quarantine email release rescan	Before releasing personal/system quarantine email, an option has been added to rescan the email for virus infections, in case the antivirus database of FortiGuard and FortiSandbox has been updated.
Default recipient based policy	A default system level recipient policy is added. If enabled, the default policy will be checked first.
FortiSandbox statistics	A new chart is added on the Dashboard to display the FortiSandbox statistics.
Header From field in history log	A new column is added for email Header From.
FortiCloud certificate	Verify FortiCloud server's certificate for better security.
User preference setting in webmail	In the resource profiles, administrator can now turn off the user preference option for the webmail users.

What's Changed

FortiMail 5.4.0 GA release experiences a major GUI re-organization. Many menus, submenus and taps have been moved and reorganized.

The following table lists some of the changes, but not all of them.

Features	Descriptions
Event logs	Event logs are split into system events and mail events.
Mail directions	Removed incoming/outgoing email directions in antispam, antivirus, content profiles, and recipient based policies.
Centralized quarantine/IBE server	Centralized quarantine/IBE servers supported from FortiMail 400E/VM02 now. Previously this was only supported on 1000D/VM04 and higher platforms.
IP pool	Use IP groups instead of IP ranges in IP pool profiles.
Combined IP and recipient based policy scanning	When exclusive IP policies are not configured, combine the same type of profiles in both the IP and recipient policies. Profiles in recipient based policies take precedence. When exclusive IP policies are configured, use profiles in the IP polices;
Personal quarantine in outbound policy	When this is configured, personal quarantine email will be put under system quarantine.
Central management by FortiManager	Starting from v5.4 release, this feature is removed.

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 (Windows 7) and Edge (Windows 10)
- Firefox 52 to 54
- Safari 9 to 10 (Mac OS X)
- Google Chrome 53 to 59

Recommended browsers on mobile devices for webmail access

- Official Safari browser for iOS 9 to10
- Official Google Chrome browser for Android 5 to 7

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 5.2.3

↓

5.2.3 (Build 436)

↓

5.2.8 (Build 467)

↓

5.3.10 (Build 643)

↓

5.4.0 (Build 692)

For any 4.x release

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)

↓

5.4.0 (Build 692)

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 5.4.0 to 5.x or 4.x releases

Downgrading from 5.4 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 5.4 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.

Antivirus/antispam/content

Bug ID	Description
437437	In some cases, FortiMail releases email before getting query results from FortiSandbox.
438974	DKIM signing of an already DKIM signed email renders the new signature invalid.
439502	Email bodies with Cyrillic text should not be detected by content profiles as audio files.
440016	DLP profiles are unable to identify DEA numbers in email bodies or attachments.
440804	Dictionary entries are counted incorrectly if searched in headers.
408432	Heuristic scanning fails to detect spam contents in PDF files.
399692	Antispam scanning still continues after safelist word matches if FortiSandbox is enabled.
405044	DLP profiles catch email incorrectly as profanity.
399237	"Replace content" and "convert HTML to text" features in the content profile do not work correctly.
414313	Mailfilterd crashes when no sensitive data selected in DLP rules.
400352	Custom replacement messages are not used in the attachment scan rules in the content profiles.
400309	Unable to send mail with EICAR test file attachments when the session profile has "Enable DKIM signing for outgoing message" selected.
405784	Antivirus is not applied to the LDAP routed email.
407142	Spam email should not be delivered after the "personal quarantine" action.
404865	Antispam block list/safe list entries should not be allowed to exceed the maximum value when added via CLI.
400175	Spoofed senders are not handled properly.
404734	Microsoft Excel files with protect workbook are detected as password protected MS Office files.
404474	DKIM signature fails verification for some users.
435030	Notification email is only sent to one of the multiple recipients when the recipient addresses are rewritten by the content profile action.
422538	Some file types may cause mailfilter exceptions.
423539	On some low end platforms, email messages that trigger spam outbreak protection may take longer time to get released.

Bug ID	Description
442073	When a virus infection is detected, the notification email does not show the virus risk level.
404903	SURBL should not catch hyperlinked IP addresses.
438279	FortiMail should inform FortiCloud once a submission to cloud sandbox is timed out.

MTA/Proxy

Bug ID	Description
398661	SMTP recipient verification command "RCPT TO:" fails with Microsoft Office 365.
424557	In some case, FortiMail delivers two versions of the same email to the users.
424547	Delivery failure handling "Minimum time for delayed email in queue" is not honored.
408176	Access control in the advanced MTA control settings does not take effect until the mailfilterd is restarted.
412122	Maximum number of attachment and maximum level of compression settings in content profiles do not work properly.
411080	Local part in RCPT TO: should not be converted to lower cases.
405784	Antivirus is not applied to the routed mail by LDAP.
405406	Content filter can be bypassed by sending an email message as RTF with winmail.dat attachment.

System

Bug ID	Description
402479	FortiMail v5.4.0 is no longer vulnerable to the following CVE references: CVE-2016-9317 CVE-2016-6912 CVE-2016-10166 CVE-2016-10167 CVE-2016-10168 CVE-2016-5766 CVE-2016-6132 CVE-2016-6207 CVE-2016-6128 CVE-2016-5767 CVE-2015-8874
436186	Variables used for "Envelope From:" in the custom email notification template is not effective.
437401	FortiMail-VM sends shortened/wrong domain name for DNS queries.
423280	Use X-XSS-Protection HTTP secure header to block reflected XSS attacks.
438279	FortiMail should inform FortiCloud once a submissionto to cloud FortiSandbox times out.

Bug ID	Description
414068	XSS vulnerability under customized webmail login page.
439730	VMSF_DELTA filter in unrar allows arbitrary memory write.
411505	Blocks "Reverse Tabnabbing" attack.
441032	Upgraded Apache httpd daemon.
399803	Newfoundland time zone shows NST instead of NDT.
384220	FortiMail does not support two factor authentication.
414592	Contacts without email addresses cannot be synchronized via CardDAV.
405399	User renaming does not work properly.
408987	Unable to view certain folders on NAS storage after upgrading to v5.3 release.
408287	FortiMail does not respond to SNMP v3 requests from SolarWinds Orion.
424531	S/MIME sign is logged but skipped if the encryption action is "encrypt and sign" and the recipient certification is not available.
406190	RADIUS access profile override does not work in some cases.
403371	Port 6688 is open publicly.
403161	When the HA slave is synchronizing greylist database from the master, an error message was recorded and the greylist cannot be displayed on the slave GUI.
417578	In HA mode, remote SMTP checking should not take priority over slave port monitoring for master election.
412441	Daylight saving is not counted when sending time zone information to FortiCloud.
434615	Added a time zone for Namibia.

Log and Report

Bug ID	Description
404712	When selecting Mail Statistics under Log and Report > Report Settings, both Mail Statistics and Statistics are selected.

Admin GUI/Webmail

Bug ID	Description
408438	Configuring an email group as sender pattern in a recipient policy on the GUI changes the "set sender-domain" in CLI from * to a random domain.

Bug ID	Description
400566	In webmail, forwarded email does not show the CC field in the original message data.
406133	Inline forwarding of an email message with attachments in webmail breaks the attachment file names.
421272	When doing a search under Monitor > Log, only one search result tab opens. Any succeeding search results will overwrite the single tab.
415749	When attaching a file in webmail, the message blocked by antivirus is not displayed properly.
442065	Email attachments with multipart/AppleDouble content type cannot be displayed in webmail.
393451	Admin GUI will not be accessible after trying to log in with an extra long admin name.

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