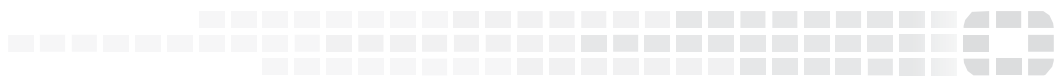




FORTINET

High Performance Network Security



FortiMail™ Release Notes

VERSION 5.4.9 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



March 29, 2019

TABLE OF CONTENTS

Change Log.....	4
Introduction	5
Supported Platforms	5
What's Changed	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
Firmware downgrade.....	9
Downgrading from 5.4.9 to 5.x or 4.x releases.....	9
Resolved Issues	10
Antispam/Antivirus/Content	10
Mail Receiving/Delivery	10
Common Vulnerabilities and Exposures	10
System	10
Log and Report.....	11
Admin GUI/Webmail	11
Known Issues	12
Image Checksums	13

Change Log

Date	Change Description
2019-03-29	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 5.4.9 release, build 741.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400C
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000C
- 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 Changed

The following table summarizes the behavior changes in this release.

Features	Descriptions
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.

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

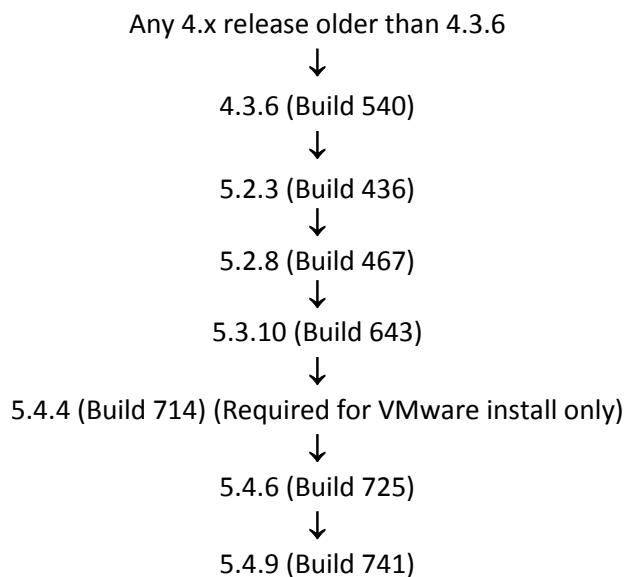
For security reasons, starting from 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, challenge/response should be used.

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



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 5.4.9 to 5.x or 4.x releases

Downgrading from 5.4.9 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 5.4.9 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
518789	Invisible characters may cause dictionary and banned word scan not working.
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.
528389	In some cases, spam email may cause error messages.
531333	Unable to decompress certain tar files.
546154	Too many log messages are generated when encoding fails.
545276	Phishing URIs in large PDF attachments cannot be detected.
547671	Dictionary profiles cannot detect and block banned words in Office 365 Word files.
545921	DKIM does not work properly when the email has multiple recipients.

Mail Receiving/Delivery

Bug ID	Description
531152	FortiMail drops connections for email that contains specially formatted HTML parts.
527130	A distribution list can only be expanded to a maximum of 1500 recipients.

Common Vulnerabilities and Exposures

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

Bug ID	Description
524928	FortiMail 5.4.9 release is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">● 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.

Bug ID	Description
529670	IP pools are not working after upgrading from 5.4.3 to 5.4.8 release.
531574	Intermittent issues with DNS and recipient verification.
525772	In some cases, mailfilterd may cause high CPU usage.
540909	LDAP nested group search does not work with cache enabled.
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.
538111	IBE user password typo resets confirmation web page.
513719	Archive Email Search is not working when using "Index and message search" type.
544856	Smtppqd memory leak.

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.
538398	Report values are inconsistent.

Admin GUI/Webmail

Bug ID	Description
525639	Some description column in the custom messages are empty.
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.
524858	Configurations of smart identifiers in a dictionary profile are reset to default after the dictionary profile is modified.
525436	Webmail SSO does not redirect to the IDP after logging out.
546543	The printer page opens automatically while trying to view the system quarantine page.

Known Issues

The following table lists some minor known issues. .

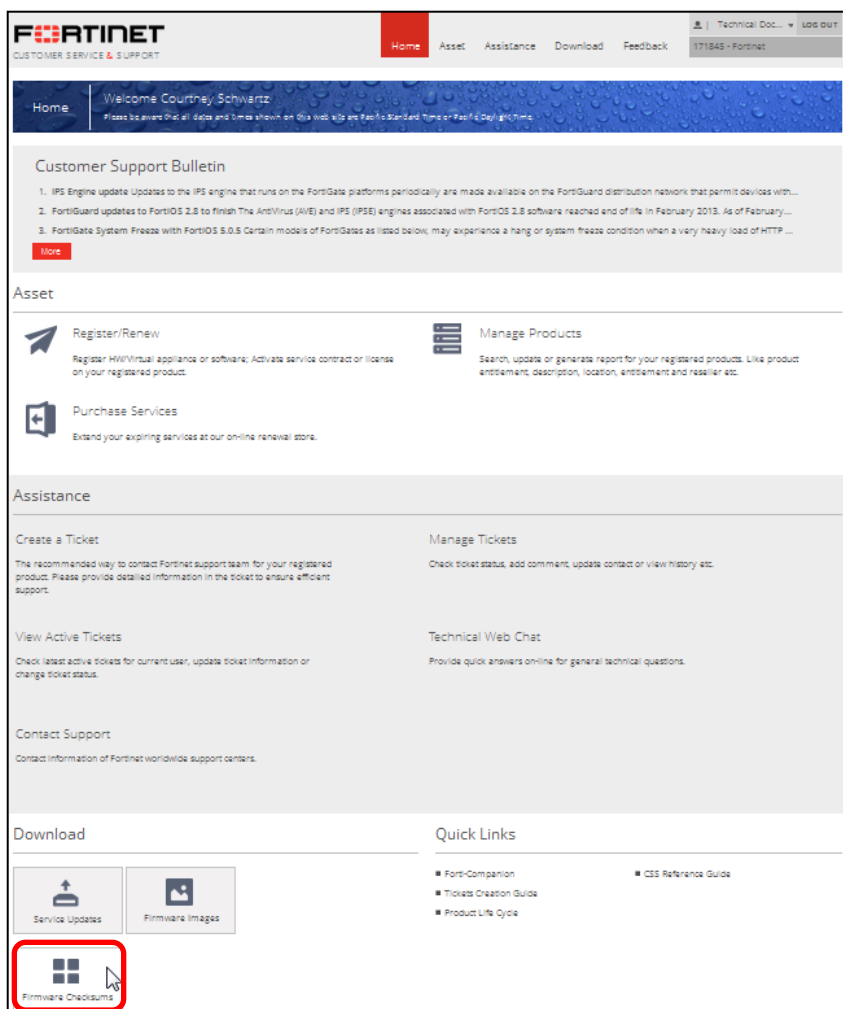
Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

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.

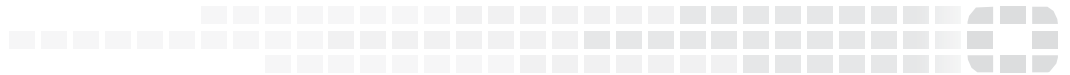
MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support 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© 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.