FortiMail - Release Notes

Version 6.0.9

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 TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 30, 2020
FortiMail 6.0.9 Release Notes
06-609-000000-20200330

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-03-30	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.9 release, build 167.

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

There are no new features introduced in this patch release.

Special notices

This section highlights the special notices that should be taken into consideration before upgrading your platform.

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 the 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 access

- Internet Explorer 11 and Edge 44, 80
- Firefox 68.5 ESR, 73
- Safari 12, 13
- Chrome 80

Recommended browsers for mobile devices for webmail access

- Official Safari browser for iOS 11, 13
- Official Google Chrome browser for Android 8.0 to 10

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 and downgrade

Before any firmware upgrade or downgrade, save a copy of your FortiMail configuration by going to **Dashboard > Status** and click **Restore** in the **System Information** widget.

After any firmware upgrade or 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. Also go to verify that the build number and version number match the image loaded.

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.

Firmware downgrading is not recommended and not supported in general. Before downgrading, consult Fortinet Technical Support first.

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) > **6.0.9** (build 167)

Firmware downgrade

Firmware downgrading is not recommended and not supported in general. If you need to perform a firmware downgrade, follow the procedure below.

1. Back up the 6.0.9 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 inquires about a particular bug, please contact Fortinet Customer Service & Support.

Antispam

Bug ID	Description
576743	Safelisted words are identified correctly in email header.
605136	In some cases, URLs in email body cannot be detected and sent to FortiSandbox for further scanning.
612696	In the content profile, when the first attachment scan rule action is set to none, the remaining scan rule actions are not followed.
613405	Fortimail 6.2.3 should not do SPF check against RFC 1918 private IP addresses.
618632	When a DKIM signed email is system quarantined then released, the DKIM verification will fail due to invalid body hash.
616649	Looped SPF record causes Mailfilterd termination.
607713	Email attachments are incorrectly classified by the content filter.
621615	Bayesian training from archive account does not work.
621806	Sender rate control should not be triggered by spoofed inbound email.

Mail delivery

Bug ID	Description
619752	When Domain Relay is MX Record (alternative domain), FortiMail queries the alternative domain MX record on the primary DNS server instead of the alternative domain's internal DNS server.
620942	In transparent mode, notification email which is supposed to sent to the sender is sent to the recipient's server instead.

System

Bug ID	Description
617064	Dead mail is not removed when the retention period has passed.
610868	Unable to view all the contents when opening an attachment from the quarantine.
607948	CMDB error when cloning domain level antispam or content filter profiles in 6.2 releases.
612052	Memory leak in FortiMail 32-bit 6.0 release.
615105	System quarantine folders are not deleted after they pass the configured retention period.
608247	In some cases, LDAP authentication does not work for newly configured domains.
607519	Multiple continuous URL links without characters in email content may cause mailfilterd to stop working.
610878	Quarantined email in the quarantine folder are not deleted after they pass the configured retention period.
607720	SNMP community setting does not support IP subnet input.

Admin GUI and webmail

Bug ID	Description
609935	Webmail mail folders with Cyrillic characters cann't be opened or created.
608687	The local disk usage value of the archived email displays differently between CLI and Web UI.

Log and report

Bug ID	Description
608176	No log is recorded when a quarantined message is opened and released from System Quarantine.
611496	In some cases, deleting email from quarantine is not logged.
614742	Inaccurate Top Spam IP report.

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.
(No bug ID)	Due to more confining security restrictions imposed by the iOS system, email attachments included in IBE PUSH notification messages can no longer be opened properly on iOS devices running version 10 and up. Therefore, users cannot view the encrypted email messages on these iOS devices. Users should download and open the attachments on their PCs as a workaround.