FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 6.0.5 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 23, 2019

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-04-23	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.5 release, build 0148.

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 Changed

The following table summarizes the behavior changes in this release.

Features	Descriptions
URI filter action change	Before 6.0.5 release, if the URI filter action is triggered, no more other antispam scanning will be done. After 6.0.5 release, if the URI filter action is triggered but the action is not final, other antispam scanning will continue.
Reference URIs	To reduce false-positives, URIs without scheme, such as example.com, will not be queried anymore, because they are not clickable.
NTP server	Changed default NTP server from pool.ntp.org to ntp1.fortiguard.com and ntp2.fortiguard.com.

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)

↓

6.0.5 (Build 148)

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 6.0.5 to 5.x or 4.x releases

Downgrading from 6.0.5 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 6.0.5 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
518789	Invisible characters may cause dictionary and banned word scan not working.
549961	Not DKIM signature is generated when Mail From is empty but the Header From is not.
549420	False positive in DLP sensitive data scan.
544827	In some cases, low-risk URIs are not replaced as configured.
543019	URI click protection removes Japanese characters.
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.
530592	MilterException errors when doing disclaimer insertion.
551451	Under Security > Quarantine > System Quarantine Setting, the account name field should only allow to enter the local part of an email address, not the entire email address.

Mail Receiving/Delivery/IBE

Bug ID	Description
542901	When a large number of IBE users try to access their encrypted email simutaniously, some users may experience problems to register and access their email.

System

Bug ID	Description
542637	Fortinet VM appliance anti-exploit enhancement.
540341	Configurations are not synchronized when FIPs in enabled in a Config Only HA cluster.
550525	When upgrading from 5.4 to 6.0.4 release, the Mail Queue permission in the user defined admin profile is always set to none. Instead, it should inherit from the Policy permission.
551408	Wrong certificate chain is supplied when the default certificate is chained and the IP pool is used.
540909	LDAP nested group search does not work with cache enabled.

Bug ID	Description
544856	Smtpqd memory leak.

Log and Report

Bug ID	Description
542735	Cached logs are not sent to remote log server FortiAnalyzer after FortiMail loses connection to FortiAnalyzer for a few hours.

Admin GUI/Webmail

Bug ID	Description
546543	The printer page opens automatically while trying to view the system quarantine page.
552338	The warning sign in the content disarm and reconstruction message cannot be displayed properly in Internet Explorer.

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