FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 6.0.7 GA

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 COOKBOOK

https://cookbook.fortinet.com

FORTINET TRAINING SERVICES

https://www.fortinet.com/training

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

October 24, 2019

TABLE OF CONTENTS

Change Log 4
Introduction 5
  Supported Platforms 5
What's New 6
What's Changed 7
Special Notices 8
  TFTP firmware install 8
  Monitor settings for web UI 8
  Recommended browsers on desktop computers for administration and Webmail 8
  Recommended browsers on mobile devices for Webmail access 8
  FortiSandbox support 8
  SSH connection 8
Firmware Upgrade/Downgrade 9
  Before and after any firmware upgrade/downgrade 9
  Upgrade path 9
  Firmware downgrade 10
    Downgrading from 6.0.7 to 5.x or 4.x releases 10
Resolved Issues 11
  Antispam/Antivirus/Content/Session 11
  Mail Receiving/Delivery 11
  System 11
  Admin GUI/Webmail 11
  Common Vulnerabilities and Exposures 12
Known Issues 13

Change Log

Date	Change Description
2019-10-01	Initial release.
2019-10-21	Added CVE-2019-15712.
2019-10-24	Added CVE-2019-15707.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.7 release, build 0160.

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

This release has no new features.

What's Changed

The following table summarizes the behavior changes in this release.

Features	Descriptions
Local search	Added search box for safelist/blocklist at System/Domain/User level.
Telnet removal	Removed telnet from help message for authserver track.

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 60.8 ESR, 68
- Safari 12
- Chrome 75

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)

↓

6.0.7 (Build 160)

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 6.0.7 to 5.x or 4.x releases

Downgrading from 6.0.7 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 6.0.7 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/Session

Bug ID	Description
579873	Messages from non-zero day IP are incorrectly delayed in spam outbreak queue.
578380	Email content was garbled after inserting disclaimer at start of message with antispam profile action or content profile action.

Mail Receiving/Delivery

Bug ID	Description
585078	FortiMail failed to parse the url in the mail body.
577630	Address mapping does not work when disclaimer is enabled.
574096	There is mail delivery issue after upgrade.

System

Bug ID	Description
537335	Having “Reject different SMTP sender identity” enabled does not check the domain part when the FROM is a protected domain.
586345	Inserting Disclaimer into certain email causes large swap files.
580480	Administrators should not be allowed to log in with HTTP GET method.
579574	New IBE users are unable to register.
570751	CDR (URL Protection) removes the space between the lines and is received as text.
574342	LDAP group with access-control policy does not work after upgrade.
579253	Read only Admin Profile has Read-Write Access.

Admin GUI/Webmail

Bug ID	Description
584428	History log disposition field has wrong "Insert Disclaimer" message.
576017	Admin GUI has issue with displaying history log.

Common Vulnerabilities and Exposures

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

Description
FortiMail 6.0.7 is no longer vulnerable to the following CVE-Reference: • CVE-2019-10092 • CVE-2019-10098 • CVE-2019-10082 • CVE-2019-10081 • CVE-2019-9517 • CVE-2019-10097 • CVE-2019-15712 • CVE-2019-15707

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.