FortiMail - Release Notes

Version 6.0.12

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

November 30, 2021
FortiMail 6.0.12 Release Notes
06-6012-08-0764535-20211130

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Supported platforms 5
What's new **6**
Special notices **7**
TFTP firmware install 7
Monitor settings for the web UI 7
Recommended browsers 7
FortiSandbox support 7
SSH connection 8
Firmware upgrade and downgrade **9**
Upgrade path 9
Firmware downgrade 9
Resolved issues **10**
Antispam/Antivirus 10
Mail delivery 10
System 10
Log and Report 11
Admin GUI and Webmail 11
Common vulnerabilites and exposures 11
Known issues **12**

Change Log

Date	Change Description
2021-11-30	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.12 release, build 183.

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 major new features 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

For desktop computers:

- Microsoft Edge 95
- Firefox 94
- Safari 15
- Chrome 95

For mobile devices:

- Official Safari browser for iOS 14,15
- Official Google Chrome browser for Android 11, 12

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) > **6.0.12** (build 183)

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 6.0.12 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

Bug ID	Description
707494	In some cases, FortiMail gets no results from FortiSandbox for some email.
740683	SPF records using macros are not handled properly.
754271	Outbound email from FortiMail Cloud occasionally fails DKIM check.
756824	Return code from DNSBL events of spamhaus.org is not handled properly.
758378	Disclaimer Insertion action is logged but no disclaimer is inserted in the email.
660873	Too many impersonation analysis false positives under certain conditions.
735742	DKIM check failure caused by DKIM signature format.
709825	Fail to detect files with .js extension included in BZIP2 archives.

Mail delivery

Bug ID	Description
747525	Authentication-Results header placement doesn't follow RFC7601.
752912	In some cases, a single email may be sent to personal quarantine numerous times.

System

Bug ID	Description
757174	When some LDAP profiles have network connection issues, all LDAP profiles may not work properly.
720374	When importing users from a .csv file, users cannot log in to their accounts.

Bug ID	Description
755862	If the mail data is scheduled to be backed up with one copy only, the new backup does not overwrite the old ones.
743949	When the full config file is backed up via TFTP, the file cannot be decompressed correctly.
712577	PDF attachment scan may cause High CPU usage.
725014	Same as above.
681597	Same as above.

Log and Report

Bug ID	Description
733781	When the relay server is unreachable, the log message "relay=" field displays the domain name, instead of the relay host name or IP address.
718183	Too many "Cannot resolve remote server" log messages.
755988	Header From and To fields in history log only support a maximum of 128 characters.
758521	Missing event log and SNMP trap for RAID events.

Admin GUI and Webmail

Bug ID	Description
756496	SNMP trap and query options are missing from the GUI when adding SNMP communities and users.
724125	In some cases, mail bodies may not be displayed in system quarantine or webmail.

Common vulnerabilites and exposures

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

Bug ID	Description
690201	CWE-20: Improper Input Validation
697129	CWE-287: Improper Authentication
692463	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

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. ***Note***: This issue has been fixed in 6.4.0 release.
594547	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.