



**FORTINET**  
High Performance Network Security



# FortiMail™ Release Notes

VERSION 5.4.12 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](mailto:techdocs@fortinet.com)



# 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 web UI.....	7
SSH connection.....	7
Product Integration and Support.....	8
FortiSandbox support .....	8
AV Engine .....	8
Recommended browsers .....	8
For desktop computers: .....	8
For mobile devices.....	8
Firmware Upgrade/Downgrade.....	9
Before and after any firmware upgrade/downgrade .....	9
Upgrade path .....	9
Firmware downgrade.....	10
Downgrading from 5.4.12 to 5.x or 4.x releases .....	10
Resolved Issues .....	11
Antispam.....	11
Mail Delivery .....	11
System .....	11
Admin GUI/Webmail .....	11
Known Issues .....	12

# Change Log

Date	Change Description
2020-09-24	Initial release.

# Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 5.4.12 release, build 0751.

## 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 2.12.1 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 New

There are no new features in this patch release.

## 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.

### 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.

# Product Integration and Support

## FortiSandbox support

- FortiSandbox 2.3 and above

## AV Engine

- Version 5.00355

## Recommended browsers

### For desktop computers

- Microsoft Edge 44, 84
- Firefox 80
- Safari 13
- Chrome 85

### For mobile devices

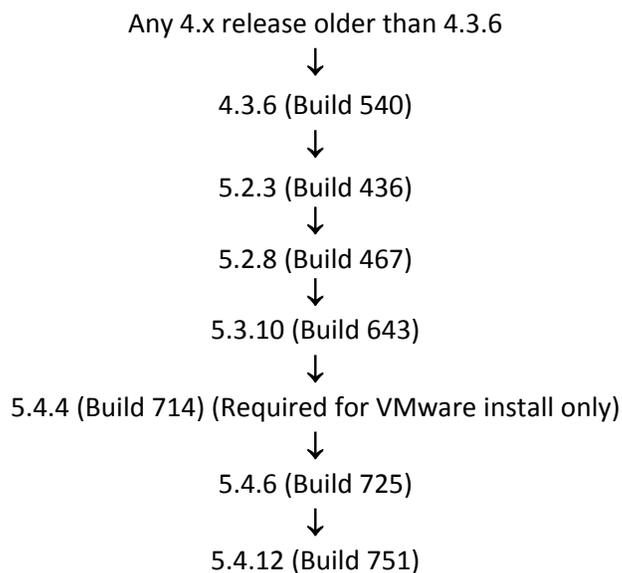
- Official Safari browser for iOS 13
- Official Google Chrome browser for Android 9, 10

# 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 5.4.12 to 5.x or 4.x releases

Downgrading from 5.4.12 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 5.4.12 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 inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

### Antispam

Bug ID	Description
607519	Multiple URL links without characters in email body may cause mailfilterd to stop running.
612696	Attachment file filter execution order issue.
602218	Performance improvement when identifying DMARC policy record changes. .
612683	In some cases, when the content profile is configured to remove URLs in email HTML part, the email may be rejected.

### Mail Delivery

Bug ID	Description
602236	In transparent mode, DSNs are delivered to the clients instead of the server of the protected domain.
658706	Connections may drop when receiving mail with archive attachments from Microsoft Exchange servers.

### System

Bug ID	Description
538398	When a report is generated multiple times with same conditions, some values in the reports are not consistent.
612052	Memory leak in 32-bit releases.

### Admin GUI/Webmail

Bug ID	Description
603056	After the end of year 2019, the old email displays wrong dates in the webmail email list.
609935	After upgrading, webmail mail folders with Cyrillic characters cannot be opened or created any more.

## 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.

**FORTINET**

*High Performance Network Security*



Copyright© 2020 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.