



Release Notes

FortiMail 7.0.6



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



April 5, 2023

FortiMail 7.0.6 Release Notes

06-706-895099-2023-04-04

TABLE OF CONTENTS

Change Log	4
Introduction and Supported Models	5
Supported models	5
What's New	6
Special Notices	7
TFTP firmware install	7
Monitor settings for the web UI	7
SSH connection	7
Product Integration and Support	8
FortiSandbox support	8
Fortisolator support	8
AV Engine	8
Recommended browsers	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 Vulnerabilities and Exposures	11

Change Log

Date	Change Description
2023-04-05	Initial release.
2023-04-19	Change to upgrade path.
2023-04-20	Added MS Hyper-V Server 2022.
2023-05-12	Added Mantis bug 913475 to Resolved Issues.

Introduction and Supported Models

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 7.0.6 release, build 216.

For FortiMail documentation, see the [Fortinet Document Library](#).

Supported models

FortiMail	200E, 200F, 400E, 400F, 900F, 2000E, 2000F, 3000E, 3000F, 3200E
FortiMail VM	<ul style="list-style-type: none">• VMware vSphere Hypervisor ESX/ESXi 6.0, 6.7, 7.0 and higher• Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2, 2016, 2019, 2022• KVM qemu 2.12.1 and higher• Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher• AWS BYOL• Azure BYOL• Google Cloud Platform BYOL• Oracle Cloud Infrastructure BYOL

What's New

The following table summarizes the new features and enhancements in this release. For details, see the [FortiMail Administration Guide](#).

Feature	Description
Microsoft OneNote Virus Detection	The new AV engine in this release starts to support OneNote virus detection.
Attachment Deferred Scan Notification Enhancement	Under <i>Security > Disarm & Reconstruction > Attachment > Attachment handling for deferred email</i> , for the notification email, added an option to include the disarmed Office/PDF attachments while removing other non-CDR supported attachments.

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.

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

Fortisolator support

- Fortisolator 2.3 and above

AV Engine

- Version 6.00287

Recommended browsers

For desktop computers:

- Microsoft Edge 111
- Firefox 111
- Chrome 111
- Safari 16

For mobile devices:

- Official Safari browser for iOS 15 and 16
- Official Google Chrome browser for Android 12 and 13

Firmware Upgrade and Downgrade

Before any firmware upgrade or downgrade, save a copy of your FortiMail configuration by going to **Dashboard** > **Status** and click **Backup** 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) > **6.0.5** (build 148) > **6.2.4** (build 272) > **6.4.5** (build 453) > **7.0.6** (build 216)

Firmware downgrade

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user accounts
- admin access profiles

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/Antivirus

Bug ID	Description
882498	Attachments with passwords containing a dot (.) cannot be decrypted.
876426	In some cases, SPF check may not work properly.
867221	Personal safelist is ignored if the safelisted sender typed the same naming schema of the internal user while sending the mail.
867667	SPF check is not performed before trusted MTA, when "Received" chain is broken.
874400	In some cases, only one antispam action is applied even though multiple non-final actions are triggered.
888208	If enabling to continue FortiSandbox scan on CDR, HTML files are not sent to FortiSandbox.
896458	Microsoft OneNote files are detected as plain/text instead of application/octet-stream by the content filter.

Mail Delivery

Bug ID	Description
880743	Some email may become expired in Microsoft 365 view.
875621	In some cases, email messages are not delivered and remain in the mail queue without any action.
873984	Released domain quarantined outbound email goes back to the sender instead of the recipient.
888653	IPv6 IP policies are not matched when the message size is above 10MB.

System

Bug ID	Description
880226	In HA mode, local mail user password change via webmail on the secondary unit does not take effect.

Bug ID	Description
876817	In HA mode, some email may not be viewable or released in the centralized monitor.
883012	In HA mode, changes to the block list and safe list via webmail on the secondary unit does not take effect.
821855	FortiMail 3K HA running 7.0.3 won't accept configuration changes via GUI or CLI.
873052	Unable to add secondary account through REST API.
893587	Domain admins cannot release multiple messages from the history log.
900005	Deleting email in system quarantine won't free up disk space.
913475	In some cases, the mailfiltered process may stop working and restart itself.

Log and Report

Bug ID	Description
873970	In some cases, log search takes longer time than usual.

Admin GUI and Webmail

Bug ID	Description
876756	The administrator list cannot be sorted by status (enabled or disabled).
868019	Error when trying to download an attachment from an email in the domain quarantine.
873551	When attaching multiple files to an email in webmail, the email body can no longer be displayed.
871670	When admin web access is disabled, new IBE user registration page displays incorrectly.

Common Vulnerabilities and Exposures

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

Bug ID	Description
889200	FortiMail 7.0.6 is no longer vulnerable to the following CWE Reference: <ul style="list-style-type: none">CWE-358: Improperly Implemented Security Check for Standard



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.