FortiMail - Release Notes

Version 7.0.2

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 23, 2021
FortiMail 7.0.2 Release Notes
06-702-760830-20211123

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-11-23	Initial release.
2022-04-14	Added v7.0.0 to upgrade path.

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 7.0.2 release, build 177.

For FortiMail documentation, see the Fortinet Document Library.

Supported models

FortiMail	200E, 200F, 400E, 400F, 900F, 2000E, 2000F, 3000E, 3000F, 3200E
FortiMail VM	• 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 • KVM qemu 2.12.1 and higher • Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher • AWS BYOL and On-Demand • Azure BYOL and On-Demand • Google Cloud Platform BYOL • Oracle Cloud Infrastructure BYOL

What's New

The following table summarizes the new features and enhancements in this release.

Feature	Description
Microsoft 365 Graph API Support	A service root endpoint for each Microsoft national cloud can now be set when configuring a Microsoft 365 connection.
Encrypted Email Access Enhancement	IBE account expiration notification email will include a self-activation link which allows IBE users to reactivate their accounts by themselves.

What's Changed

The following table summarizes the behavior changes in this release.

Feature	Description
Domain Group Size	The maximum number of domains in a domain group has been increased from 16 to 50 for all platforms.

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

AV Engine

- Version b267

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

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) > **7.0.0** (build 133) > **7.0.2** (build 177)

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 inquires about a particular bug, please contact Fortinet Customer Service & Support.

Antispam/Antivirus

Bug ID	Description
746912	Email cannot be released from user quarantine or system quarantine when sandbox re-scan is enabled.
758272	Policy lookup does not work properly when protected domain names contain capital letters.
750161	Content Monitor does not detect regular expressions in CSV attachments.
753015	Some .docx files may not be processed properly when antivirus is enabled.
756824	Return code from DNSBL events of spamhaus.org is not handled properly.
754271	Outbound email from FortiMail Cloud occasionally fails DKIM check.
758578	Disclaimer Insertion action is logged but no disclaimer is inserted in the email.
761931	OpenSSL encrypted files (.enc files) are not detected by the correct file type.

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.
752043	The initial SMTP greeting message 220 is sent after about 4 seconds, instead of instantly.

System

Bug ID	Description
757174	When some LDAP profiles have network connection issues, all LDAP profiles may not work properly.
746856	Unable to resize FortiMail disk in Azure.

Bug ID	Description
754949	FortiMail spam sample submission outlook plugin is not installed for all user accounts on a PC.
747569	In active-passive HA mode, when disabling admin/web access to one port, access to another port may also be disabled.
749800	IBE one-time secure token is resent every time when the IBE user refreshes the IBE secure token authentication page.
752950	Upgrade issue from 6.0.x to 6.2.x releases.
755862	If the mail data is scheduled to be backed up with one copy only, the new backup does not overwrite the old ones.
758276	LDAP Domain Mail Host does not work properly with associated domains.
743949	When the full config file is backed up via TFTP, the file cannot be decompressed correctly.
758805	After upgrading from 6.2.4 to 6.4.5 release, the config-only HA primary unit is reset to standalone.
758521	No event logs or SNMP traps for RAID events.
747073	SMTP traffic cannot pass through WCCP tunnel between FortiMail and FortiGate.
755603	After upgrading from 6.4.4 to 7.0.1 release, SMTP recipient verification is lost.
756748	After upgrading 6.4.5 release, there is a problem accessing the quarantine via webmail.

Log and Report

Bug ID	Description
755080	After upgrading from 6.4.5 to 7.0.1 release, domain administrators can view logs of other non-assigned domains.
759715	Log search by client name/IP does not work properly.
755988	Only 128 characters/symbols are supported in Header From and To log fields. The maximum has been increased to 350 now.

Admin GUI and Webmail

Bug ID	Description
756748	After upgrading to 6.4.5 release, the quarantine web access URL stopped working in some cases.
757084	Webmail access cannot be completely disabled.
756496	SNMP trap and query options are missing from the GUI when adding SNMP communities and users.
759279	Quarantine email content can still be viewed even when viewing content detail is disabled.

Common vulnerabilites and exposures

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

Bug ID	Description
753903	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').