FortiMail - Release Notes

Version 6.2.8

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

January 21, 2022
FortiMail 6.2.8 Release Notes
06-628-774577-20220121

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-01-21	Initial release.

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 6.2.8 release, build 291.

Supported models

FortiMail	60D, 200E, 200F, 400E, 400F, 900F, 1000D, 2000E, 3000E, 3200E
FortiMail VM	• VMware vSphere Hypervisor ESX/ESXi 5.0 and higher • Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2, 2016, 2019 • KVM qemu 0.12.1 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

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 6.2.165

Recommended browsers

For desktop computers:

- Microsoft Edge 97
- Firefox 96
- Safari 15
- Chrome 97

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 **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) > **6.0.5** (build 148) > **6.2.8** (build 291)

When upgrading from 6.2.7 to 6.4 release, you must upgrade to 6.4.5 and newer releases, not other older 6.4 releases.

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 6.2.8 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
770841	URL exemption for domain names does not work with aggressive URI-checking.
758378	Disclaimer Insertion action is logged but no disclaimer is inserted in the email.
754271	Outbound email from FortiMail Cloud occasionally fails DKIM check.
756824	Return code from DNSBL events of spamhaus.org is not handled properly.
761931	OpenSSL encrypted files (.enc files) are not detected by the correct file type.
753015	Some .docx files may not be processed properly when antivirus is enabled.
740683	SPF records using macros are not handled properly.
737742	DKIM verification may fail due to DKIM signature format reasons.
738397	In some cases, FortiMail fails to allow text/plain attachments.

Mail Delivery

Bug ID	Description
712202	User-defined variables cannot be used in email templates.
752912	In some cases, a single email may be sent to personal quarantine numerous times.
747525	Authentication-Results header placement doesn't follow RFC7601.
752047	The initial SMTP greeting message 220 is sent after about four seconds, instead of instantly.
700997	Error message when sending email in batches with more 25 recipients.

System

Bug ID	Description
757174	When some LDAP profiles have network connection issues, all LDAP profiles may not work properly.
752950	Upgrade issue from 6.0.x to 6.2.x releases.
770916	Unable to configure distinguished name (DN) with more than 127 characters.
755862	If the mail data is scheduled to be backed up with one copy only, the new backup does not overwrite the old ones.
747569	In active-passive HA mode, when disabling admin/web access to one port, access to another port may also be disabled.
743949	When the full config file is backed up via TFTP, the file cannot be decompressed correctly.
729955	Incorrect Japanese translation in custom messages.
725014	High CPU usage when scanning PDF files.
587729	Traffic capture duration setting does not work properly.
731620	AWS VM license will be disabled after a few hours as duplicate by getting code 401.
728065	High CPU due to the "expireenc" process.
727609	Updating an LDAP password that does not meets the LDAP server's password policy returns a wrong message at FortiMail webmail.
766819	Mail data gets corrupted after transferred to a NAS device.
765128	In server mode config-only HA, multiple calendar event reminders are sent to users.
745733	Failed to check certificate revocation status when validating FortiAnalyzer's server certificate.
731620	In some cases, AWS VM license might be disabled as duplicate.

Log and Report

Bug ID	Description
755988	Increase the log field length of From and To in history logs.
758521	Missing event log and SNMP trap for RAID events.
758617	No system event log is created for power supply issues.
733781	Logs do not display the relay host/IP properly.

Admin GUI and Webmail

Bug ID	Description
757084	Webmail access cannot be completely disabled.
756496	SNMP trap and query options are missing from the GUI when adding SNMP communities and users.
768328	In gateway mode, sub-domain based administrators with read & write access cannot access domain based settings.
729564	When replying all in webmail, the sender email is also included in the recipient list.
724125	The body of MIME email with non-standard HTML is not displayed in system quarantine and webmail.

Common Vulnerabilities and Exposures

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

Bug ID	Description
771106	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
686309	CWE-329: Not Using a Random IV with CBC Mode
753903	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
690201	CWE-20: Improper Input Validation
697129	CWE-287: Improper Authentication

Known Issues

The following table lists some minor known issues.

Bug ID	Description
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. This issue has been resolved in FortiMail v7.0.0 release.