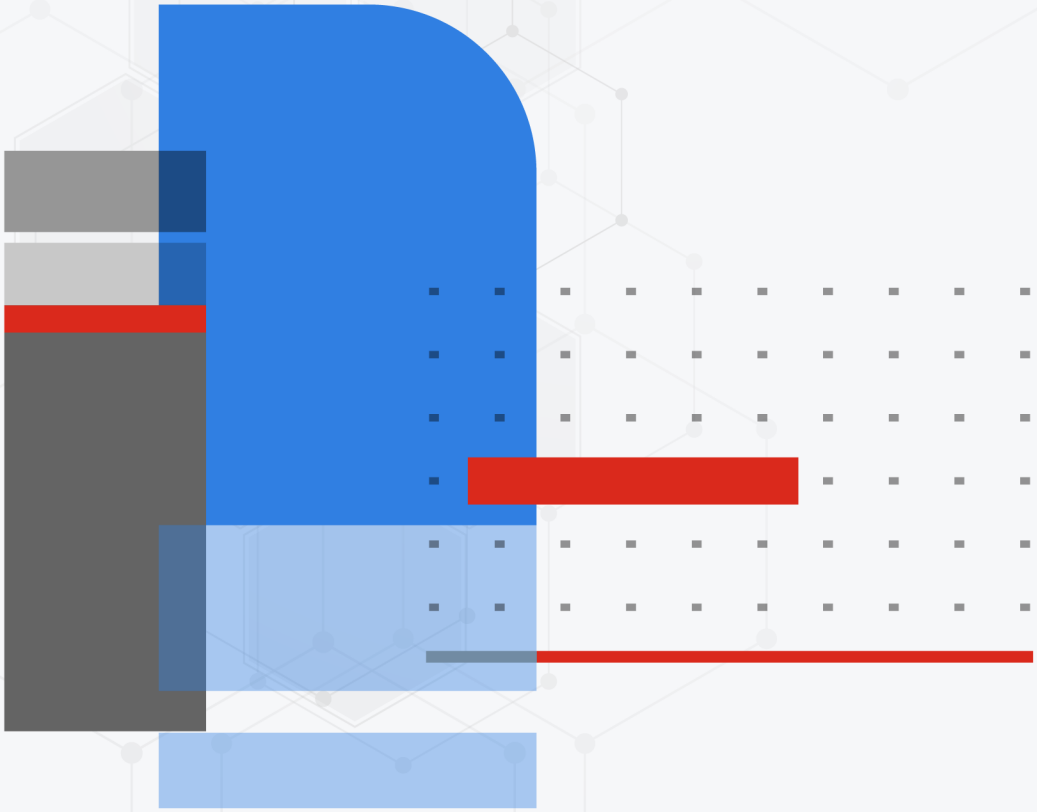
Release Notes

FortiMail 7.2.3



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 18, 2023
FortiMail 7.2.3 Release Notes
06-723-894637-20230418

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-04-18	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 7.2.3 release, build 395.

For FortiMail documentation, see the Fortinet Document Library.

Supported models

FortiMail	200F, 2000E, 2000F, 3000E, 3000F, 3200E, 400F, 900F
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, 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 and On-Demand • 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.

Impersonation Analysis Levels	Added the following CLI command to control the IA strictness:
	`config antispam settings`
	`  set impersonation-analysis-level {aggressive | strict}`
	`end`
	For details, see the FortiMail CLI Reference.

Attachment Deferred Scan Notification Enhancement	Under *Security* > *Disarm & Reconstruction* > *Attachment* > *Attachment handling for deferred email*, for the notification email, added an option to include the disarmed Office/PDF attachments while removing other non-CDR supported attachments.
New VM Platform Support	AWS on-demand is supported starting from this 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 1280 x 1024.

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

- Version 2.3 and above

FortiNDR support

- Version 7.0.0

FortiIsolator support

- FortiIsolator 2.3 and above

FortiAnalyzer Cloud support

- Version 7.0.3

AV Engine

- Version 6.00287

Recommended browsers

For desktop computers:

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

For mobile devices:

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

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) > **7.2.3** (build 395)

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
882498	Attachments with password containing a dot (.) cannot be decrypted.
876426	In some cases, SPF check may not work properly.
890410	DKIM results are not recorded in the Authentication-Results header.
867221	Personal safelist is ignored if the safelisted sender typed the same naming schema of the internal user while sending the mail.
859815	In some cases, impersonation exemption may be ignored.
858117	In some cases, PDF attachment scan detects URL incorrectly.
867667	SPF check is not performed before trusted MTA, when "Received" chain is broken.
876061	In some cases, HTML links in an email may be incorrectly removed.
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.
902812	Personal quarantine mail cannot be released when the mail subject is encoded.
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.
888653	IPv6 IP policies are not matched when the message size is above 10MB.
873984	Released domain quarantined outbound email goes back to the sender instead of the recipient.

System

Bug ID	Description
880226	In HA mode, local mail user password change via webmail on the secondary unit does not take effect.
876817	In HA mode, some email may not be viewable or released in the centralized monitor.
860445	Unable to release email from the folders under system quarantine.
883012	In HA mode, changes to the block list and safelist via webmail on the secondary unit does not take effect.
858690	When a global inbound disclaimer is inserted in an email with text/calendar content type, the body of the email is not displayed.
893587	Domain admins cannot release multiple messages from the history log.
900005	Deleting email from system quarantine won't free up disk space.
821855	FortiMail 3K HA running 7.0.3 won't accept configuration changes via GUI or CLI.
901891	Associated domain user data is not backed up with CLI command "execute formatmaildisk-backup".
903260	A system reboot is required for DMARC report settings to take effect.
880313	In some cases, insert disclaimer action does not work properly.
913475	In some cases, the mailfilterd process may stop working and restart itself.

Log and Report

Bug ID	Description
876785	When a new mail statistics report is created with a specific sender domain, the report may keep loading when editing.
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).
890913	Domain admins cannot view release logs under release log search.
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.

Bug ID	Description
871670	When admin web access is disabled, new IBE user registration page displays incorrectly.
869331	After upgrading to v7.2.2, the domain section does not allow ordering by MTA status.

Common Vulnerabilities and Exposures

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

Bug ID	Description
889200	FortiMail 7.2.3 is no longer vulnerable to the following CWE Reference: • CWE-358: Improperly Implemented Security Check for Standard

Known Issues

The following table lists the known issues that will be fixed in future patch releases.

Bug ID	Description
906766	After upgrading to FortiMail Cloud v7.2.3 release, the block/safe lists are missing and it's unable to add new entries to the lists. The workaround is to reload the FortiMail instance, back up the lists under *System* > *Maintenance* > *Block/Safe List Maintenance*, and then restore the lists. This issue has been resolved in v7.2.4 release.

www.fortinet.com