FortiMail - Release Notes

Version 6.2.5

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 24, 2020
FortiMail 6.2.5 Release Notes
06-625-652130-20200724

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-07-24	Initial release.
2020-12-09	Added more detailed description to scan levels in What's New.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.2.5 release, build 278.

Supported platforms

- FortiMail 60D
- FortiMail 200E
- FortiMail 200F
- FortiMail 400E
- FortiMail 400F
- FortiMail 900F
- FortiMail 1000D
- FortiMail 2000E
- 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 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher)
- FortiMail VM (AWS BYOL and On-Demand)
- FortiMail VM (Azure BYOL and On-Demand)

What's new

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

Feature	Description
Dictionary and DLP scan levels	Three levels of low, medium, and high in the CLI commands (`config mailsetting mail-scan-options`) to control the aggressiveness of the dictionary and DLP scan rules. The higher the level, the more aggressive the scan, and thus more resources are required. The default setting is medium. In older releases, the setting is equivalent to low.
GeoIP group	Able to include all countries/regions when creating a GeoIP group.

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.

Recommended browsers on desktop computers for administration and webmail access

- Microsoft 44, 83
- Firefox 78
- Safari 13
- Chrome 84

Recommended browsers for mobile devices for webmail access

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

FortiSandbox support

- FortiSandbox 2.3 and above

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.

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) > **6.2.5** (build 278)

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 6.2.5 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
647719	Not all email messages are released from quarantine when more than one message is selected.
645940 649702	Sender alignment can be bypassed by invalid email addresses.
643822	Policies with IPV6 address groups are not triggered when enforced authentication uses IP policies.
645726	File signatures containing uppercase letters cannot be detected in antivirus file signature check.
637306	Disclaimers are not inserted in matching DLP profiles.
637785	URL Click Protection does not work in Config-HA (A-A) scenarios due to Base URL replication.
639591	Outlook cannot display single quotation marks in email when Click Protection is enabled.
637980	When MAIL FROM is empty, EHLO hostname is checked for SPF.
524641	Base64 escaped UTF-8 strings in the Header From address followed by a valid sender will be accepted.
618993	Email with empty body cannot be blocked.
635846	Adding and deleting entries in the DLP fingerprint file list does not work properly.
629247	Dictionary profile import fails if any of the entries has a comment field configured in two lines.
624567	Some URLs may not be rewritten with URL click protection.
624159	File filters can be lost in cloned content profiles.
628785	Open XML files with passwords should not be detected by MS PowerPoint application type.
625381	In some cases, disclaimer insertion does not work properly.
627919	Changes to an email group won't take effect in the access control rule until the rule is disabled and enabled.
631873	DLP Profile is incorrectly triggered by a Microsoft Word document with no credit card information in it.

Mail delivery

Bug ID	Description
647405	When relay type is configured as "LDAP Domain Mail Host" and "Mail Routing Profile" is used, the corresponding IP policy uses the configured IP Pool in internal-to-internal mail traffic. .
630390	Original email is sent to the archive account twice.
640136	Associated domains are not shown in the address mapping domain list.

System

Bug ID	Description
647701	When using LDAP chaining and the chained LDAP profile has cache enabled, users cannot be found in the cache.
514185 645950	In some cases, Cyrillic alphabet from some domains shows incorrect encoding.
639448	IP addresses are logged in Incorrect log fields in the sessions rejected by IP policies.
636342	Fail to mount archive file system in some cases.
637815	Reports stops to generate due to incorrect memory usage calculation.
628789 632039	Regular expression scan may cause high CPU usage.
612685	Wildcards in dictionary profiles may cause high CPU usage.
624620	Large PDF attachments may cause high CPU and memory usage.
623103	Under some conditions, the mailfilterd may cause high CPU usage.

Admin GUI and webmail

Bug ID	Description
645059	Images embedded in email body are lost when resending the email in webmail.
637186	Importing CSV contact lists in webmail doesn't work.
649504	When replying to an IBE message that has the display name separated by a comma with umlauts, the display name cannot be displayed properly.
623774	Oversized passwords should not be allowed when adding new administrators.

Bug ID	Description
632335	Access Control rule status is not changed when changed via Preview in Advanced Control in a session profile.

Common vulnerabilites and exposures

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

Bug ID	Description
637249	Crafted user name cannot trigger login attempt limits.

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. This has been fixed in 6.4 and newer releases.
(No bug ID)	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.

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.