



FortiMail - Release Notes

Version 6.2.6

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/support-and-training/training.html>

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 19, 2020

FortiMail 6.2.6 Release Notes

06-626-678372-20201119

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported platforms	5
Special Notices	6
TFTP firmware install	6
Monitor settings for the web UI	6
SSH connection	6
Product Integration and Support	7
FortiSandbox Support	7
AV Engine	7
Recommended browsers	7
Firmware Upgrade and Downgrade	8
Upgrade path	8
Firmware downgrade	8
Resolved Issues	9
Antispam/Antivirus	9
Mail delivery	9
System	9
Admin GUI and webmail	10
CLI	10
Known Issues	11

Change Log

Date	Change Description
2020-11-19	Initial release.
2021-06-22	Removed 200D from the supported platforms.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.2.6 release, build 282.

Supported platforms

FortiMail	60D, 200E, 200F, 400E, 400F, 900F, 1000D, 2000E, 3000E, 3200E
FortiMail VM	<ul style="list-style-type: none">• VMware vSphere Hypervisor ESX/ESXi 5.0 and higher• Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2, 2016• 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 6.00153

Recommended browsers

For desktop computers:

- Microsoft Edge 86
- Firefox 83
- Safari 14
- Chrome 86

For mobile devices:

- Official Safari browser for iOS 13, 14
- Official Google Chrome browser for Android 10, 11

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) > **6.2.6** (build 282)

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 6.2.6 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 inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Antispam/Antivirus

Bug ID	Description
677857	DOC files uploaded into DLP sensitive data fingerprint are not detected.
667425	DOCX files uploaded into DLP sensitive data fingerprint are not detected.
662953	Invalid URLs in email may cause email rejection.
673226	In some cases, DMARC checking may fail for some domains.
669438	Email classified as "TLS Session" shouldn't be counted as spam in spam reports.
666868	ISO attachments are not detected by file MIME type.
660487	Spam outbreak protection stops working when access control receiving policies are matched.
660873	Impersonation analysis false positive issue.
624567	Some URLs may not be rewritten with URL click protection.

Mail delivery

Bug ID	Description
673911	DSNs should have the host name instead of the client IP address in EHLO.
663329	In some cases, FortiMail transparent mode intermittently stops passing traffic.
658706	The mailfilterd may exit while trying to decrypt archive attachments.

System

Bug ID	Description
673962	After upgrading to 6.2.5 release, email aliases cannot log on to webmail anymore.

Bug ID	Description
675831	Some email attachment types may cause high CPU usage.
669689	No DSNs are sent after the email in queue reaches the maximum time.
669983	In some cases, recipient verification over SMTPS may cause high CPU usage.
669152	Administrator idle timeout does not work for REST API login.
663290	When email address parsing mode is set to relaxed, gateway mode also loosens LDAP recipient verification and allows non-existing hosts.
660143	In some cases, customized email templates may be set to default.
655958	When the remote archive server is not reachable, the mail queue may cause high disk usage.
654451	In some cases, mailfilterd may cause high CPU usage.
659393	Changes to LDAP alias options are not reflected on the GUI.
660878	External IBE users cannot change their user information under Preferences settings.
656401	IP Pools disappear from access control delivery policies on config HA secondary unit after certain configuration changes.
630571	After rebooting the config HA secondary unit, it cannot synchronize properly with the primary unit.

Admin GUI and webmail

Bug ID	Description
662754	When sending an encrypted email, image files may not be attached in some cases.

CLI

Bug ID	Description
653179	The "execute erase-filesystem" command returns wrong partition size information.

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.
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.



Copyright© 2021 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.