FortiMail - Release Notes

Version 6.2.9

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

September 15, 2022
FortiMail 6.2.9 Release Notes
06-629-841779-20220915

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-09-15	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 6.2.9 release, build 294.

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 • Azure BYOL

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 6.00165

Recommended browsers

For desktop computers:

- Microsoft Edge 105
- Firefox 104
- Safari 15
- Chrome 105

For mobile devices:

- Official Safari browser for iOS 15
- Official Google Chrome browser for Android 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) > **6.2.9** (build 294)

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 6.2.9 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.

System

Bug ID	Description
786272	Disclaimers are not added even when "Insert disclaimer" is enabled.
778938	"Attempt to decrypt archive" and "Words in e-mail content" does not decrypt .zip files.
707515	The secondary unit in an active-passive HA mode cannot recover from out-of-sync mode with checksum mismatch.
817272	Issue with HA synchronization due to certificate checksum mismatch.
781956	Events of adding user safe and block list via webmail are missing from System Event logs.
768328	Sub-domain administrators cannot view domain settings in gateway mode.
672299	The dnscached process may cache incorrect query results under heavy traffic.

Common Vulnerabilities and Exposures

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

Bug ID	Description
776309	CWE-121: Stack-based Buffer Overflow
824889	Curl library upgrade: CVE-2022-22576 CVE-2022-27782 CVE-2022-30115 CVE-2022-27781 CVE-2022-27780 CVE-2022-27779 CVE-2022-27776 CVE-2022-27775 CVE-2022-27774

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.