Release Notes

FortiMail 7.6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 29, 2025
FortiMail 7.6.2 Release Notes
06-762-1016106-20250829

TABLE OF CONTENTS

Change log **4**
Introduction and supported models **5**
Supported FortiMail models 5
Special notices **6**
Communication between HA secondary units 6
HA heartbeat and DHCP 6
TFTP firmware install 6
Monitor settings for the web UI 6
SSH connection 7
FortiGuard Web Filtering category v10 update 7
What's new **8**
Product integration and support **10**
FortiNDR integration 10
FortiIsolator integration 10
FortiAnalyzer Cloud integration 10
FortiGuard Antivirus Engine 10
Recommended browsers 10
Firmware upgrade and downgrade **12**
Upgrade path 12
Firmware downgrade 12
Resolved issues **13**
Antispam/antivirus 13
System 13
Logs and reports 14
Administrator GUI/webmail 14
Common Vulnerabilities and Exposures 15

Change log

The following is a list of documentation changes. For a list of software changes, see the other contents of this document.

Date	Change Description
2025-01-30	Initial release of FortiMail 7.6.2 Release Notes.

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 7.6.2 mature release, build 773.

For more FortiMail documentation, see the Fortinet Document Library.

Supported FortiMail models

FortiMail	200F, 400F, 900F, 2000E, 2000F, 3000E, 3200E, 3000F
FortiMail VM	• VMware vSphere Hypervisor ESX/ESXi 7.0, 8.0 and later • Microsoft Hyper-V Server 2016, 2019, and 2022 • KVM qemu 2.12.1 and later • Citrix XenServer v5.6sp2, 6.0 and later; Open Source XenServer 7.4 and later • Alibaba Cloud BYOL • AWS BYOL and On-Demand • Azure BYOL and On-Demand • Google Cloud Platform BYOL • Oracle Cloud Infrastructure BYOL

Special notices

This section highlights the special notices that should be taken into consideration before upgrading your platform.

Communication between HA secondary units

Due to the introduction of primary backup in active-active HA in FortiMail 7.4.0, communication between the secondary units is also required. In config-only HA before FortiMail 7.4.0, it was not required.

HA heartbeat and DHCP

If you upgrade from FortiMail 7.4.2 or earlier, and if the HA heartbeat's network interfaces have dynamic addresses such as DHCP, then you must either:

- before the upgrade, use static IP addresses instead
- after the upgrade:
  a. Immediately log in to all units in the cluster.
  b. Re-configure the heartbeat interfaces with their current IP addresses from the DHCP server.
  c. Reset the primary/secondary role if necessary, so that only one unit is the primary.

Cloud deployments (such as on Microsoft Azure) may commonly or by default use DHCP, requiring this setting change or procedure.

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 GUI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280 x 1024.

SSH connection

For security reasons, starting from the FortiMail 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, a challenge and response should be used.

FortiGuard Web Filtering category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency web sites. In order to use the new categories, customers must upgrade their Fortinet products to one of the versions below.

- FortiMail 7.0.7, 7.2.5, 7.4.1 or later

What's new

The following table summarizes the new features and enhancements in this release. For details, see the FortiMail Administration Guide and FortiMail CLI Reference.

Feature	Description
FortiFlex Support	Support FortiFlex on VM platforms. FortiFlex (formerly Flex-VM) is a subscription service to configure and manage VM usage entitlements. For information, see https://docs.fortinet.com/product/flex-vm/24.4.
Click Protection Statistics	Added a new tab under *FortiView* > *Threat Statistics* > *Click Protection Statistics* to display a summary of the most clicked URLs in the last 30 days.

Bare Line Feed Handling	Added the following CLI command to specify how to handle bare line feeds (also known as SMTP smuggling). The default setting is `allow`, which is the same behavior as before.
	`config system mailserver`
	`  set smtp-eom-bare-lf-handling {allow | disallow | ignore}`
	`end`

Mail Queque Delivery Control	Added CLI commands (under `config system mailserver`) to control email queue delivery attempts.

Reliable Logging to FortiAnalyzer	Added reliable logging to FortiAnalyzer with the following CLI command:
	`config log setting remote`
	`  edit <name>`
	`  set reliable {enable | disable}`
	`  end`
	`end`

Sender Identity Check for Authenticated Users	Email will be allowed as long as the mail's envelope (Mail From:), header (From:), and authenticated user name have the same DN on the configured LDAP server.
Policy Lookup Enhancement	Added policy search and display enhancements under *Policy* > *Recipient Policy* > *Inbound* and *Policy* > *Recipient Policy* > *Outbound*.

FortiGuard HTTP Proxy Setting Enhancement	Added FQDN support for the proxy with the following CLI command:
	`config system fortiguard antivirus`
	`  set tunneling-address <ip-or-fqdn>`
	`end`

Log Search Enhancement	Added a log level filter to log search.
Recipient Verification Enhancement for Email Continuity Enabled Recipient	Added an option under domain level to override the system setting to provide more granularity when configuring the recipient verification mode.
IBE User Password Reset by Administrator	Added a button for the administrators to reset the IBE user passwords under *Domain & User* > *IBE User* > *Active User*.

Feature	Description
Member Search for Group Profiles	Added a group member search function in group profiles and all the relevant pages where the group profiles are applied.
Drag & Drop Support for Attachment Upload in Webmail	In addition to the attachment icon, webmail users can now drag & drop files as email attachments.

Product integration and support

FortiNDR integration

- FortiNDR 7.0.0

FortiIsolator integration

- FortiIsolator 2.3 and later

FortiAnalyzer Cloud integration

- FortiAnalyzer Cloud 7.0.3

FortiGuard Antivirus Engine

- Version 7.00025

Recommended browsers

The FortiMail GUI has been tested on the following web browsers for computers:

- Apple Safari 17
- Google Chrome 131
- Microsoft Edge 131
- Mozilla Firefox 133

For mobile devices:

- Official Google Chrome browser for Android 14
- Official Safari browser for iOS 17

Other browser versions have not been tested, but may fully function.

Other web browsers may function correctly, but are not supported by Fortinet.

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

6.0.5 (build 148) > **6.2.4** (build 272) > **6.4.5** (build 453) > **7.0.6** (build 216) > **7.2.2** (build 380) > **7.4.3** (build 600) > **7.6.2** (build 773)

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
1098766	Messages with URLs redirecting to phishing sites cannot be caught.
1094034	In some cases, DMARC check won't fail although DMARC alignment fails.
1086798	In some cases, legitimate email may be caught as spam due to QR code check failure.
1100219	Not all URLs in the email are sent to FortiSandbox.
1111258	Match all condition "Body is Empty" and "Empty subject regex" in the DLP profile is not triggered.
1115693	When creating a scheduled scan in the MS365 API view, the advanced condition is ignored.
1115188	After upgrading to FortiMail 7.6.0/7.6.1 release, CDR mistakenly inserted download link of the original file.
1119272	PDF attachments are not detected by the content filter when regular expressions are used to match URLs in PDFs.
1119624	Content filter fails to detect regular expression/pattern matches in PDF archives.

System

Bug ID	Description
1090327	DMARC report will not be generated when RUA `mailto` domain doesn't match the sender domain.
1069702	FortiMail broadcasts with destination port 8014.
1088864	In HA mode, SAML SSO is synchronized from the primary to secondary unit, causing login failures on the secondary unit.
1066090	SNMP traps cannot be sent for the deferred mail queue threshold.
1087752	In active-active HA mode, SNMP OIDs show the wrong HA roles.

Bug ID	Description
1094863	Failure to add internal domain for alert email due to strict domain checking
1098759	Address book disappeared after upgrading to FortiMail 7.6.0/7.6.1 release.
1100041	Failure to release or delete email using quarantine reports in Gmail.
1082373	High CPU usage and increasing FortiSandbox mail queue.
1103297	Failure to add new users in some cases.
1082843	After upgrading to FortiMail 7.6.1 release, the smtpd server may terminate when there is an antivirus DB update going on.
1104413	High CPU usage caused by mailfilterd .
1107735	Failure to release system quarantined email.
1111271	Dictionary profile names remain after restoring an older config not containing the profiles.
1107717	"remote_wildcard" administrator is able to create administrator accounts but unable to delete them.
1076001	Some SSH key exchange algorithms should be removed when strong crypto is enabled.

Logs and reports

Bug ID	Description
1078550	Quarantine report is garbled when special characters are used in the email subject and "remove-active-content" is enabled.
1079025	In some cases, the log search task does not work properly.
1105759	Log message "timed out checking block safe lists" is misleading.
1114308	Domain access level log view does not work as expected for administrator accounts.

Administrator GUI/webmail

Bug ID	Description
1086810	In some cases, IBE password reset/reactivation URL does not work.
1069966	Unauthorized FortiMail units are displayed as FortiVoice in the FortiGate Security Fabric.
1075043	Support Ukrainian alphabet ordering.
1086806	Threat feed malware hash files are not read correctly.

Bug ID	Description
1097114	Multiple logins are required to access IBE email.
1101465	In some cases, HTML mail content cannot be displayed properly.
1110158	After upgrading to FortiMail 7.6.1, an error message "Invalid E-Mail Address" appears when sending email using an address book contact in FortiMail webmail.
1115801	Webmail session timeout does not respect the idle timeout setting.
1089762	Scheduled reports are delivered later than expected.

Common Vulnerabilities and Exposures

FortiMail 7.6.2 is no longer vulnerable to the following CVE/CWE-References.

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

Bug ID	Description
1081109	CWE-400: Uncontrolled Resource Consumption
1092958	CWE-23: Relative Path Traversal

www.fortinet.com