Release Notes

FortiMail 7.2.0

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

May 10, 2022
FortiMail 7.2.0 Release Notes
06-720-803372-202205010

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-05-10	Initial release.
2022-06-02	Added a note to What's New.
2024-04-09	More details about webfilter local category support in What's New.

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 7.2.0 release, build 338.

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 • KVM qemu 2.12.1 and higher • Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher • AWS BYOL • 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
FortiNDR (FortiAI) Integration	FortiNDR malware detection server has been integrated into the antivirus profile.
FortiAnalyzer Cloud Integration	FortiMail can send logs to FortiAnalyzer Cloud.
Email Continuity Enhancements	• Internal email: Captures internal-to-internal email for Email Continuity. • BCC self: Added "BCC self" option to Email Continuity in resource profile. • Address book synchronization: LDAP address book can be synchronized to FortiMailat configured intervals. • Authentication improvements.
Mail Queue Search Enhancement	Added sending, deleting, and delivering to alternative host functions in mail queue search. Also added REST API support for these functions.
Quarantined Email Attachment Download Control	Added control in the resource profile to disable/enable webmail users' attachment download of their personal quarantines.
Authenticated Received Chain (ARC) Support	Support ARC validation and sealing.
Header Removal	Added header removal to content and DLP action profiles.
Configuration Control	Added CLI commands to restrict domain level admins to make changes to some settings.
Redirector URL Enhancement	Try to resolve all URLs to their final destinations.
Classifier Variables	Added classifier variables to notification message templates and increased notification profiles for some models.
Mail Routing Relay Type	Added mail host as the relay type to mail routing in MTA Advanced Control.
DMARC Enhancement	Use DMARC record's policy and take corresponding actions.
Support MTA-STS	Support MTA-STS domain checking.
MSSP Advanced Management Features	• Per domain statistics: In addition to system level mail statistics, per domain statistics metrics can be generated and viewed. • Intra domain protection: Both incoming and outgoing recipient policies can be applied between protected domains of different tenants. • New attribute fields for customer management: some domain admin settings can only be configured by system admin.
Recipient Verification	Added "discard" action to recipient verification failures.

Feature	Description
Web Filter Local Category	Support web filter local categories and rating override under *Security* > *URL Filter* > *Local Category* and *Security* > *URL Filter* > *Override Rating*. In previous releases, CLI command "`config antispam url-fgas-exempt-list`" is used to configure the URL exempt list. Starting from 7.2.0 release, CLI command "`config system webfilter local-rating`" will be used instead.
Maturity Levels of GA Releases	New GA releases will be tagged as "Maturity" or "Feature" release. The Feature tag indicates that the firmware release includes new features. The Maturity tag indicates that the firmware release includes no new, major features. Maturity firmware will contain bug fixes and vulnerability patches where applicable.
New Variables in Quarantine Summary	Added "ORIG_ENVOLOPE_TO" and "ORIG_TO" (Header To) to quarantine summary reports.
External Email Warning	Added an option in incoming disclaimers for external email only.
Description Fields	Added description/comment fields to some settings.
REST API Rate Limit	Added rate limit control to REST API access.
CLI Access Control	Added privilege levels to access CLI in admin profiles.
Utility Menu	Grouped a few utilities under System menu. • Added .msg to .eml converter • Added regular expression validator
MAIL FROM Customization	Added option to customize Mail From attribute under SMTP Recipient Address Verification in domain settings.
Block/Safe List Tracking	Added auto aging and retention option to the block/safe lists.
Replacement Custom Message Enhancement	Separate replacement messages for body and attachment parts.
URL Neutralization	Added URL neutralization action to CDR and content profile actions.
FortiSandbox URL Submission Exception	Added option to bypass one-time URLs.
DSN EHLO/HELO Argument Customization	The DSN EHLO/HELO argument can be set to host name, domain name, or other customized name. The default is host name.
URL Checking	Resolve URLs to their final destinations before FortiGuard query.
New `execute factoryreset2` Command	Reset the FortiMail unit to its default settings for the currently installed firmware version, while retaining all network settings.
MS365 Protection	• Added individual actions for IP reputation in MS365 antispam profiles. • Added sender and recipient filtering. • When set to on-policy-match, Microsoft 365 History, Mail Event, Antivirus, and Antispam log entries will only be logged upon policy match.

Feature	Description
Load Balancer	Support load balancer on Azure and Oracle Cloud platform.

IP Pool Behavior Change	(Same feature as introduced in 7.0.3) The following CLI command has been added to control IP pool usage.
	`config system mailserver`
	`    set ip-pool-direction [ all | exclude-internal-to-internal]`
	`end`
	With the new "exclude-internal-to-internal" option, the IP pools will not be applied to the internal-to-internal email. The default setting is "all".

SSO Workflow Enhancement	Workflow and GUI enhancements.

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

- Version 2.3 and above

FortiNDR support

- Version 7.0.0

FortiAnalyzer Cloud support

- Version 7.0.3

AV Engine

- Version 6.4, build 273

Recommended browsers

For desktop computers:

- Microsoft Edge 100
- Firefox 99
- Safari 15
- Chrome 100

For mobile devices:

- Official Safari browser for iOS 14，15
- Official Google Chrome browser for Android 11，12

Firmware Upgrade and Downgrade

Before any firmware upgrade or downgrade, save a copy of your FortiMail configuration by going to **Dashboard > Status** and click **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) > **7.0.0** (build 133) > **7.2.0** (build 338)

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
782699	Email scanning continues after the final action has been taken.
782367	DLP condition "body is empty" should be applied to the email that looks empty (with invisible characters).
783166	SPF check fails for MS365 API mail.
770190	DKIM checking may not work properly in some cases.
773494	Manipulated MIME headers may bypass AV scan.
778938	In some cases, zip files cannot be decrypted.
772298	After upgrading from v7.0.1 to v7.0.2, DLP scan does not work properly.
771118	Sender IP address is added to authentication reputation blocklist after delivering five to 10 email messages.
770566	Malicious URLs in text format may bypass FortiGuard URL filter check.
770445	DLP scan does not detect words in the headers and footers of Microsoft Word documents.
770841	URL exemption for domain names does not work properly with "aggressive" URL checking.
764802	Dictionary profile was triggered with no matching pattern.
785327	DKIM check fails incorrectly.
784305	In some cases, the content filter fails to detect HTML attachments.
789214	DKIM check is not performed if the sender is in the safelist.
794309	Final action of DMARC is not applied.
792507	Quarantine report does not work for associate domains when using domain recipient policy with regular expressions.
799789	DKIM check false positive.
803094	Content filter with wildcard patterns cannot detect Thai language.
797391	In some cases, URL Click Protection does not work properly.

Mail delivery

Bug ID	Description
773010	Successful bounce verification scan does not remove the tag.
774758	DSNs are sent using the mail routing profile of the original email.
732598	In some cases, email delivery may be delayed after Microsoft 365 real-time scanning.
800994	Outbound email messages are rejected due to timeout but are logged as Accept.

System

Bug ID	Description
781056	After upgrading from v6.4 to v7.0, FortiGuard antispam service is displayed as not reachable although the service is disabled.
783656	DANE check 2.x.x should ignore "Unable to get CRL".
672299	The dnscached process may cache incorrect query results under heavy traffic.
773356	Missing deployment package for VMware ESXi 7.02.
771913	Domain disclaimers do not work properly.
768275	IP pools in ACL rules should have higher priority over IP pools in policies.
772318	Push update does not work properly.
769748	System encounters reboot loop with subscription license.
770916	Unable to configure distinguished name (DN) with more than 127 characters.
765128	In server mode config-only HA, multiple calendar event reminders are sent to users.
764216	When ping access is disabled on an interface, ping6 from FortiMail cannot be sent.
768328	Subdomain-based admins with read/write access privilege are not able to view domain based settings.
786272	In some cases, disclaimers are not added properly although the logs show otherwise.
788629	Associated domains should use the primary domain's Bayesian database.
782368	High CPU usage after upgrading from v6.4.5 to v6.4.6.
793149	Fail to subscribe MS365 users due to large number of invalid users.
781108	High memory usage caused by hasyncd.
797330	Disclaimers are not added at the top of email messages.
794074	If post-login banner is enabled on the admin portal, SSO login does not work.

Bug ID	Description
766819	Mail data may get corrupted when transferred to a NAS device.
798144	Problem with system time when using GMT time zone.
799920	Admin profile with permission to Traffic Capture cannot sniffer via CLI.
801861	High memory usage over time.

Log and Report

Bug ID	Description
781956	When adding a safe/block list via webmail, the entries are added successfully but the event is not logged.
786675	No System Event logs are generated when creating/deleting a DKIM key pair.
797621	In some cases, log search does not work properly.

Admin GUI and Webmail

Bug ID	Description
781054	History log search by message ID does not work.
777084	Sender Reputation search filter does not work with relationship set to "or".
764729	In server mode, the "Failed to open mailbox" error message may display when a webmail user tries to open a mail folder.
786646	Unable to create safelists and blocklists.
786675	No system event logs are generated when creating/deleting a DKIM key pair.
799549	Webmail GUI is blocked when composing an email message and trying to edit a link.
801157	System time section shows vertical format in Japanese GUI.
803220	FortiMail product icon is not shown on webmail GUI in server mode.
794341	IBE notification for new user registration and activation is in English while the language is set to German.
804982	On the log search page, the "Load Previous Setting" button does not repopulate the Client IP field.
804855	Admin login page is accessible from any IP address when trusted IP is set.

Common vulnerabilites and exposures

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

Bug ID	Description
776309	CWE-121: Stack-based Buffer Overflow
765178	CWE-134: Use of Externally-Controlled Format String
686309	CWE-329: Not Using a Random IV with CBC Mode
771106	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
703776	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
790809	CWE-352: Cross-Site Request Forgery (CSRF)
793937	CWE-284: Improper Access Control
773386	CWE-610: Externally Controlled Reference to a Resource in Another Sphere

www.fortinet.com