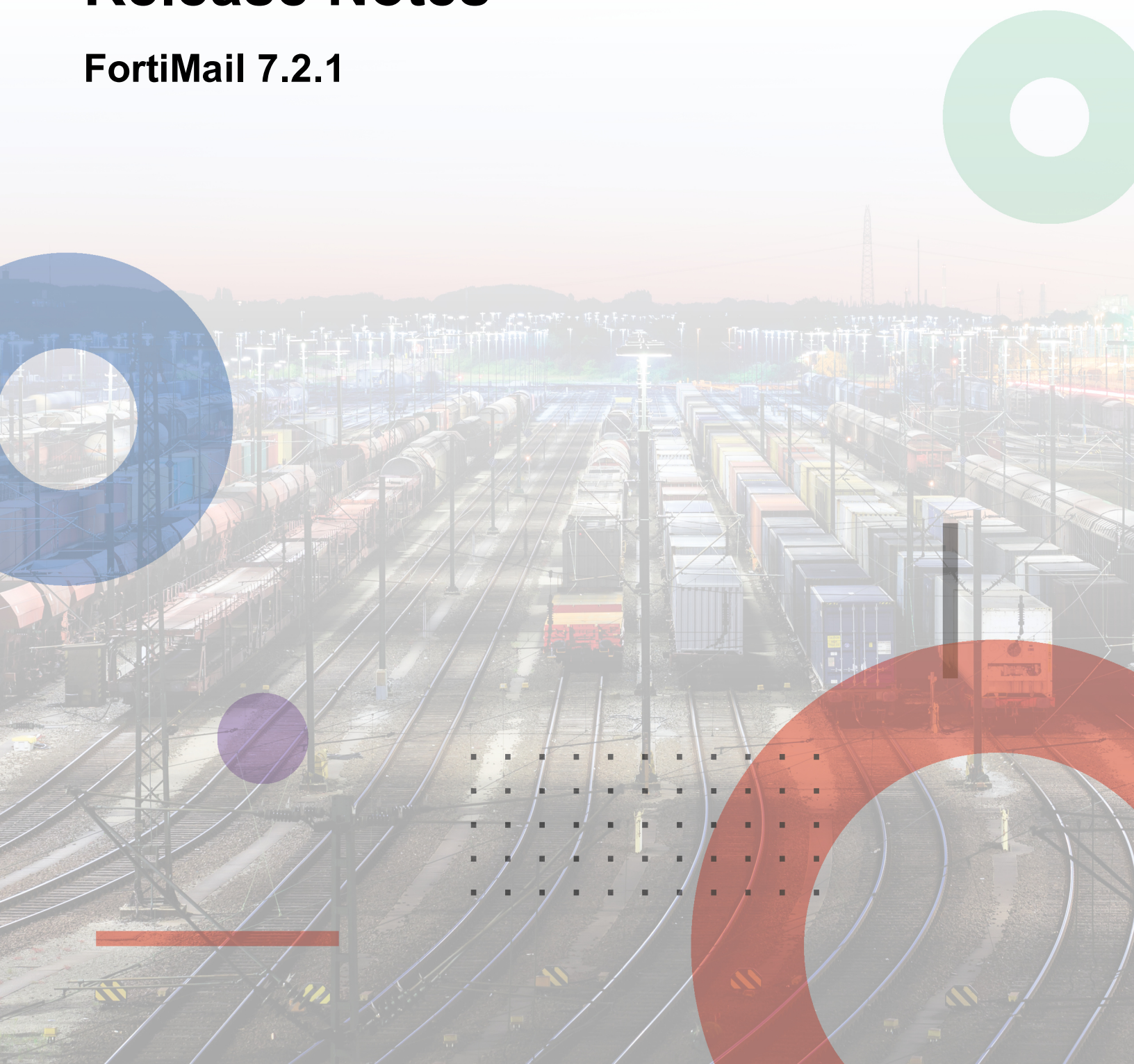
FORTINET

Release Notes

FortiMail 7.2.1



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

August 04, 2022
FortiMail 7.2.1 Release Notes
06-721-824208-20220804

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-08-04	Initial release.
2022-10-03	Added malformed HTML tag content handling enhancement to 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 7.2.1 release, build 364.

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
Business Email Compromise(BEC) Enhancements	Introduced BEC check and action in antispam profiles with BEC rules for cocktail scoring.
Granular Actions for DMARC and DKIM Scan in AntiSpam Profile	Individual actions can be configured for different DMARC and DKIM scan results.

QR Code URL Scan	Extract URLs from email body QR code images for FortiGuard and FortiSandbox scan, using the following CLI commands:
	`config antispam settings`
	`  set qr-code-url-scan-status {enable | disable}`
	`end`

Malformed HTML Tag Content Handling	The following CLI command has been added to help handling malformed HTML tag contents for URL click protection:
	`config system fortiguard url-protection`
	`  set malformed-html-tag-content-action {remove | rewrite}`
	`end`
	The default action is "remove" .

Utilize ISDB in ACL	Added Internet Service Database (ISDB) to the source type in ACL rules.
FortiSandbox Cloud EMEA Option	Added FortiSandbox Cloud EMEA region option.

DMARC Action and Antispam Profile Action Combination	FortiMail can now combine non-final actions set in the antispam profile with the actions set in the DMARC DNS record policy.
	If the antispam profile DMARC actions are non-final, such as "Tag subject" and "Notify", they are combined with the actions in the DMARC DNS record policy: None, Reject, or Quarantine.
	This happens when:
	`config antispam settings`
	`  set dmarc-failure-action use-profile-action-with-none`
	`  (and the sender's DMARC record policy is 'p=none')`
	`  Or`
	`  set dmarc-failure-action use-policy-action`
	`end`

Quarantine Search Based on Release Status	Added the release status (release or unreleased) as a quarantine search criteria.
Journaled Email Scan	Added option to scan incoming journaled email when creating a journaling source for archiving.
AWS Snowball Support	Support AWS Snowball for FortiMail KVM.

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 1280 x 1024.

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:

- Google Chrome 103
- Firefox 102
- Microsoft Edge 103
- Safari 15

For mobile devices:

- Official Google Chrome browser for Android 12
- Official Safari browser for iOS 15

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) > **7.2.1** (build 364)

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
824015	SPF check failed due to DNS look up limit reached.
815286	SPF records with macros and IPv6 client IP may cause SPF check failure.
810260	Blocklist does not work when the sending email address is between quotation marks.
813318	Client names cannot be blocked using reverse DNS patterns after upgrading to v7.2.0.
813613	When using the "Rewrite recipient email address" action, irrelevant headers are removed.
815586	URL click protection scanned by FortiSandbox takes action before timeout if action is submit only.
818127	URL rewrite is not applied to all the links in the email body.
809880	Released email from the system quarantine is quarantined again due to FortiSandbox re-scan.
811579	The block list is only applied to the first recipient.
818908	URL rewrite may not work properly in some cases.
823060	After upgrading to 7.2.0, email attachments and URIs cannot be processed properly by Fortisandbox.
822265	DKIM check fails incorrectly for valid DKIM key.
819717	Disclaimer is not added to all email messages.
811593	Two files each matched by an attachment rule with different actions ends up with only one action.
791736	In some cases, the WebFilter can only detect part of the URL.
827697	Email address starting with "."(dot) is not rejected.
824290	In some cases, a disclaimer may be duplicated when replying to an email thread.
826087	JTD files are detected as Microsoft Office files.

Mail delivery

Bug ID	Description
769015	Access control SAFE and SAFE & RELAY actions do not work on FortiMail 200E.
819657	The "for" field in the Received Header contains another recipient address when spam outbreak is triggered.
821799	Releasing email from Microsoft 365 on-demand system quarantine is delivered without the attachment.
823544	Email delivery is delayed with too many FortiSandbox mail queues.

System

Bug ID	Description
812907	Admin users have access only to the main domain but not to the associated domains after upgrading to v7.2.0.
810685	Deleting LDAP user data will not delete the user mailbox account in database.
809363	Exporting the contact group to a .csv file exports all the address book contacts.
811446	In Microsoft 365 scheduled scan and search, the "daily" setting always defaults to a 24-hour window and overwrite the other configured time periods.
692481	Custom email template variable %%ORIG_FROM%% does not work as intended.
807614	DKIM keys may get lost in some cases.
707515	The secondary unit in an active-passive HA mode cannot recover from out-of-sync mode with checksum mismatch.
821856	DNS name for remote logging cannot be resolved, resulting in no logs being forwarded.
817272	Issue with HA synchronization (certificate checksum mismatch).
823671	SSO on mobile devices does not work after upgrading to v7.0.3.
805629	Domain block/safe list tracking hit count is not displayed when NAS storage is enabled.
828856	HA synchronization issue when updating the safe/block lists.
825004	In some cases, logs show incorrect relay IP addresses.

Admin GUI and Webmail

Bug ID	Description
623544	Customer icon displayed an incorrect number of customers.
810461	The Compose Mail icon is not displayed when the mail is in the Encrypted Email folder.
813612	PKI authentication with customized webmail login page does not work.
823267	IBE webmail redirect defaults to port 443.
830963	Sorting by access level does not work under System > Administrator > Administrator.

Common vulnerabilites and exposures

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

Bug ID	Description
793937	CWE-284: Improper Access Control
826878	CVE-2022-31129: JavaScript library upgrade
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:
792100	CVE-17: OpenSSL upgrade (resolved in v7.2.0)
765178	CWE-134: Use of Externally-Controlled Format String (resolved in v7.2.0)
792533	Apache HTTPS upgrade (resolved in v7.2.0): CVE-2022-22720 CVE-2022-22719 CVE-2022-22721 CVE-2022-23943:

www.fortinet.com