FortiMail - Release Notes

Version 7.0.0

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

May 17, 2021
FortiMail 7.0.0 Release Notes
06-700-718505-20210517

TABLE OF CONTENTS

Change Log **4**
Introduction and Supported Models **5**
Supported models 5
What's New **6**
What's Changed **8**
Special Notices **9**
TFTP firmware install 9
Monitor settings for the web UI 9
SSH connection 9
Product Integration and Support **10**
FortiSandbox support 10
AV Engine 10
Recommended browsers 10
Firmware Upgrade and Downgrade **11**
Upgrade path 11
Firmware downgrade 11
Resolved Issues **12**
Antispam/Antivirus 12
Mail delivery 13
System 13
Log and Report 14
Common vulnerabilites and exposures 14
Known Issues **15**

Change Log

Date	Change Description
2021-05-17	Initial release.
2021-05-20	Minor change to What's New.
2021-05-25	Added a known issue.
2021-06-30	Modified upgrade path.
2021-09-08	Added Advanced Control changes to What's Changed.
2021-12-14	Added block/safe list enhancement to What's New.
2022-04-08	Modified Sender Alignment enhancement description in What's New.
2022-05-30	Added S-Series subscription-based pricing to What's New.
2022-07-21	Removed AWS and Azure on-demand support.

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 7.0.0 release, build 133.

For FortiMail documentation, see the Fortinet Document Library.

Supported models

FortiMail	200E, 200F, 400E, 400F, 900F, 2000E, 3000E, 3200E
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.

Feature	Description
Email Continuity	(FEEC license required) When FortiMail runs in gateway or transparent mode, end user can still interact with the incoming email when the protected mail server is not reachable.
User Account Synchronization	Periodically synchronize user accounts from the LDAP servers and MS365 servers to keep the mailbox accounting statistics up-to-date.
HA Synchronization Control	(CLI only) New CLI commands to control which settings will not be synchronized from the primary unit to the secondary unit.
HA Synchronization Status	Display HA sync status on the dashboard, centralized monitor, and HA settings.
Cousin Domain Detection	The method checks for the domain names that may be deliberately misspelled, either by character removal, substitution, and/or transposition, in order to make emails look as though they originate from trusted internal sources.
Admin Access Profile Enhancement	More detailed controls in the administrator access profiles.
DANE Support	Add DANE support to TLS profiles.
Sender Rewriting Scheme (SRS) Support	SRS is used to rewrite the envelope sender of an email address, so that emails may be forwarded by an MTA if necessary without being rejected by the receiving server which may have a strict SPF policy in place.
Larger Maximum Values	(MSSP license required) If licensed, the customer can have a larger number of domains, users, IP pools, and other controlled values.
Domain Quarantine Support	(MSSP license required) In a multi-tenant environment, a tenant can manage the quarantined messages for the specific domains.
ACL Receive Action	To combine or enforce TLS profile for inbound email, ACL Receive action is added.
Disclaimer Exclusion List Enhancement	Support IP addresses in disclaimer exclusion lists.
Block/Safe List Enhancement	Track and display blocklist and safelist statistics.
Bypass Safelist for SPF/DKIM/DMARC Check Failure	(CLI only) New command to control bypassing of safelisted senders for SPF/DKIM/DMARC check failure. When disabled, if the scan result of SPF, DKIM, or DMARC is a failure, and the sender is safelisted, the result of SPF, DKIM, and DMARC takes precedence.

Feature	Description

	`config antispam settings`
	`set safelist-bypass-sender-auth enable (default enable)`
	`end`

TLS Versions	Add TLS versions to TLS profiles.
Custom Message Enhancement	Add Message-ID variable to the disclaimer insertion message template and attachment filtering message template.
Trusted CA Certificate Download	Trusted certificate authorities certificate will be downloaded from FortiGuard. They are used to validate and sign other certificates in order to indicate to third parties that those certificates may be trusted and are authentic.
FortiSandbox and CDR Workflow Enhancement	Add more controls in CDR settings to better interact with FortiSandbox.
Email Deferral Archive	Archives the deferred email for spam outbreak, antivirus outbreak, and FortiSandbox.
Email Deferral Display	The dashboard displays the statistics of the deferred email by spam outbreak, virus outbreak, and FortiSandbox scan.
Oldest Email Archive	(CLI only) New command (`diagnose maildir archive`) to archive the oldest email in the user mailbox to improve performance and accessibility.
Log Search Enhancement	Add more search criteria when doing log search; allow to create log search tasks running at the backend for time consuming search tasks.
Quarantine Search Enhancement	Add more search criteria when doing system quarantine search.
DKIM Option in Antispam Profile	With this option, an action can be specified for DKIM check failures.
Pipelining Control	New CLI and GUI control for session pipeline.
Oracle Cloud Infrastructure (OCI) Support	New OCI platform support.
FortiSandbox Cloud Regions	Support four region settings: Global, Europe, Japan, and US.
Queue History	Add Queue History widget to the dashboard.
Sender Alignment Enhancement	Before 7.0 release, Sender Alignment checks for a Header From and Envelope From mismatch. Starting from 7.0 release, it will also check for a Header From and Reply-To mismatch.
Text File Fingerprints	Add support to text file fingerprints in DLP.
Block/Safe List Enhancement	Three block/safe list entry types are now supported: email, IP/netmask, and reverse DNS. For details, see the online help or administration guide.
Subscription-based Pricing	Released subscription-based FortiMail VM S-Series. The SKUs are available starting from v7.0.0 release and onwards.

What's Changed

The following table summarizes the behavior changes in this release.

Feature	Description
Maximum Values	Some maximum values, such as the number of admin users and domains, have been changed in v7.0.0 release. For detailed information, see the FortiMail Maximum Values on the Fortinet Documentation Library.
Advanced Control	The Advanced Control section in the session profile can now be enabled on the GUI under *System > FortiGuard > Licensed Feature > Advanced Management > Enable MTA advanced control*. Note that Advanced Control is now an option of the Advanced Management license. It is not possible to enable it without the Advanced Management license. For backward compatibility, if Advanced Control was enabled in previous releases, it will stay enabled after upgrading to v7.0.0 release, no matter the Advanced Management license is purchased or not. In future major releases, the Advanced Management license will be mandatory.

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 b262

Recommended browsers

For desktop computers:

- Microsoft Edge 88
- Firefox 88
- Safari 14
- Chrome 90

For mobile devices:

- Official Safari browser for iOS 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 **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)

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
686269	Files cannot be uploaded to FortiSanbox Cloud for inspection and all the files are incorrectly displayed with the same file size.
683293	Content filter cannot detect *.hta files for certain types of email.
681435	When "Detect on failure to decompress" is enabled in the content profile, the .zip files may cause false positives.
691329	Policy match issue with LDAP verified domains.
694038	Unable to delete dynamic impersonation database entries with special characters in the Display Name.
700919	Issues when scanning PDF files.
660873	Impersonation Analysis false positives.
684937	URL click protection does not work properly with links ending with a dot.
712099	Password protect ,7z files are incorrectly blocked.
710968	After FortiMail/FortiSandbox processes the email, the email is moved to the user's inbox, instead of the original custom folder.
709083	In some case, fail to allow PDF files.
705753	Double stamping removal only works on full domains, not on subdomains.
702148	Invalid top-level domain addresses are rejected in relaxed email parsing mode.
702940	Regular expressions are not detected in XLS files.
707494	For some email, FortiMail may get NoResult response from FortiSandbox.
709825	Fail to detect files with .js extension included in BZIP2 archives.
713087	Fail to allow Excel files when sent in .rar archives.
713397	DLP attachment metadata detection doesn't work for docx and xlsx files.
713095	Reach FortiSandbox submission limit incorrectly.
713859	Fail to detect macros in Excel legacy format *.xls files.

Mail delivery

Bug ID	Description
673911	Webmail client IP address is used in EHLO when sending DSNs for IBE reply email.

System

Bug ID	Description
688015	Cloning a used mail routing profile, when the max entries are reached, deletes the original profile.
688008	DKIM and S/MIME signing in combination does not work properly.
682822	Some GUI items are not translated into Spanish and Portuguese.
683893	Oversized email meta data is sent to FortiSandbox.
675831	The maifilterd process causes high CPU usage.
691549	After adding a new webmail custom language under *System* > *Customization* > *Appearance*, the IBE registration web portal stops working.
693194	When hide-on-email-arrival is enabled with Microsoft 365 real-time scanning, duplicate folders may be created in the mail user inbox.
690048	IBE push email enhancement.
639474	After upgrading from 6.0.7 to 6.2.4 release, the quarantine release URL in the quarantine report is incorrect on the HA config secondary unit.
700244	For Diffie-Hellman key exchange, FortiMail uses self-generated parameters, which are different from the predefined finite field groups in RFC 7919.
679151	Gmail using a "+" plus symbol for an alias causes issues with IBE account creation.
691523	Unexpected quotation marks appear in the block lists when exporting the configuration.
608247	LDAP authentication does not work for newly created domains.
683893	Oversized meta data is sent to FortiSandbox.
675831	The mailfilterd process causes high CPU usage.
705376	After upgrading from 6.4.3 to 6.4.4 release, the customized IBE language is lost.
707925	RADIUS 2FA users are locked out after the first unsuccessful login attempt.
699918	IBE customized template for 2FA secure token notification is not taking the changes on the "From" field.
691596	In FIPS-CC mode, importing a certificate via the GUI fails with the message "Unable to get certificate CRL."

Bug ID	Description
693981	Fail to connect to the SMB/CIFS server under *Data Loss Prevention* > *Sensitive Data* > *FingerPrint Source*.
692153	Same email group entries can be created due to case sensitivity.
711271	Mail authentication failed due to special characters in passwords.
692164	Possible to create identical greylist exempt entries.
712594	Disclaimers are not inserted when files are sent to FortiSandbox with Submit Only.

Log and Report

Bug ID	Description
681775	Incorrect email subject encoding modifies the cross search log lines.
707915	When certain zip files are decrypted, the action is not logged.

Common vulnerabilites and exposures

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

Bug ID	Description
694751	CWE-310: Cryptographic Issues.
695037 694752	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').
693465	CWE-36: Absolute Path Traversal.
694366	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').
691547 690894	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').
692223 697251	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').
695039	CWE-131: Incorrect Calculation of Buffer Size.
696793	CWE-325: Missing Cryptographic Step.
698764	CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG).
700991 700994	CWE-401: Missing Release of Memory after Effective Lifetime.

Known Issues

The following table lists some minor known issues which will be fixed in future patch releases.

Bug ID	Description
721171	After upgrading to v7.0.0 release, there could be issues of domain configuration loss due to the new enforced maximum number of domains for some platforms. For example, the vm02 platform can have a maximum of 100 domains in v6.4.4 release, while in v7.0.0 release, the number is 70.