FortiMail - Release Notes

Version 6.2.0

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

October 15, 2019
FortiMail 6.2.0 Release Notes
06-620-000000-20191015

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-08-09	Initial release.
2019-10-07	Added a known issue regarding TLS 1.0 support.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.2.0 release, build 249.

Supported platforms

- FortiMail 60D
- FortiMail 200E
- FortiMail 200F
- FortiMail 400E
- FortiMail 400F
- FortiMail 900F
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2, 2016)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher)
- FortiMail VM (AWS BYOL and On-Demand)
- FortiMail VM (Azure BYOL and On-Demand)

What's new

The following table summarizes the new features and enhancements in this release.

Feature	Description
MS Office 365 Active Threat Remediation	FortiMail can now perform post-delivery on-demand scan of the email on MS Office 365. Real-time scan will be added in future releases. Note that a special license is required to use this feature.
FortiIsolator integration	FortiMail is now able to participate in the security fabric with FortiIsolator. FortiMail can rewrite URLs on a per category basis to FortiIsolator for zero trust browser isolation.
Fortinet Security Fabric	Added support for the new security fabric integration using in FortiOS 6.2. Note that previous integration with FortiOS 6.0 is no longer supported.
Compliance enhancement	In order to comply with compliance standards such as GDPR, the following new features have been added: • Detail log of all configuration changes • Detail lo log of all actions performed by an admin user on queues and quarantines • Log of all search terms used
GeoIP integration	Use GeoIP database in IP policies for geography-based scanning. Also displays the GeoIP information on the GUI.
Attachment Metadata	Support DLP filtering based on attachment metadata.
TLS 1.3 support	Starting from 6.2 release, TLS 1.3 is supported for HTTPS access to FortiMail.
SSO support	In addition to webmail, SSO is also supported on admin GUI logon now.
New variables in email template	The Envelope From address and the Message-ID attribute can now be added as a variable in the quarantine report template. Local host and local domain variables can be added in the email notification template. The variable %%MESSAGE_ID%% is renamed to %%EMAIL_ID%% to avoid confusion. The email ID is assigned by FortiMail to the quarantined email while the message ID is the standard message ID in the email header.
LDAP referral and chain query	LDAP profiles now support LDAP referral and chained query.
LDAP group expansion	Added group level expansion to LDAP profile configuration. For details, see the FortiMail Administration Guide.
REST API enhancement	Added REST API commands to batch release all email in a specific system quarantine folder. Also added commands to access user level information (whitelists and blacklists).

Feature	Description
IP pool enhancement	Now you can use IP pools in ACL delivery rules.
Exempt rule for impersonation check	Now you can add exempt rule so that FortiMail will skip the impersonation check.
Search button	Added Search button on the ACL, IP Policy, and Recipient Policy pages.
IP reputation configuration enhancement	FortiGuard categorizes the blocklisted IP address into three reputation levels. Now you can specify different actions towards different reputation level of IP addresses.

What's changed

The following table summarizes the behavior changes in this release.

Feature	Description
Archive account storage quota	Instead of capping disk space for an individual account as 20% of the mail partition on the remote storage, disk usage for all the archive accounts will be capped to 80% now.
URI Click Protection enhancement	Interstitial Holding Page has been added to indicate that the page is being processed (required to notify the user to wait when longer FortiSandbox timeouts are configured).
IA scan	In addition to the Header From field, Impersonation Analysis (IA) also inspects the Reply-To field now.
IA bypass	IA will not be bypassed for ACL rule matches.
Enforce password change at first login	In order to comply with California State Law SB-327 Information privacy: connected devices, the default configuration has been changed to enforce password change on first logon.
DKIM signing	Header From domain is used for DKIM signature now. Envelope From domain was used before.
DKIM key import	Now you can import the DKIM public and private key on the GUI and encrypt the keys in the configuration file.

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.

Recommended browsers on desktop computers for administration and webmail access

- Internet Explorer 11 and Edge 42, 44
- Firefox 60.8 ESR, 68
- Safari 12
- Chrome 75

Recommended browsers for mobile devices for webmail access

- Official Safari browser for iOS 11, 12
- Official Google Chrome browser for Android 7.0 to 9.0

FortiSandbox support

- FortiSandbox 2.3 and above

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.

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) > **6.2.0** (build 249)

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 6.2.0 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.

Profiles

Bug ID	Description
569960	DLP with profanity setting does not work.
557805	Regular expressions in DLP rules and content monitor do not match contents in HTML links.
567801	For URI protection scan, FortiMail and FortiSandbox Cloud have communication issues.
568910	BCC action in the content profile does not work if DSN email generation is disabled.
567511	Rewrite From in the session profile does not work if Header From is missing.
563130	In some cases, header manipulation may not work properly.
569416	Impersonation Analysis should not be bypassed for ACL rule match.
568281	Impersonation Analysis is bypassed when an email message contains multiple recipients.
573097	When using a customized file filter in a content profile, the .pub files are caught by the MS PowerPoint filter, instead of the MS Publisher filter.
544827	In some cases, low-risk URIs are not replaced as configured.
546154	Too many log messages are generated when encoding fails.
551451	Under **Security > Quarantine > System Quarantine Setting**, the account name field should only allow to enter the local part of an email address, not the entire email address.
549961	Not DKIM signature is generated when Mail From is empty but the Header From is not.
549420	False positive in DLP sensitive data scan.
543019	URI click protection removes Japanese characters.
547671	Dictionary profiles cannot detect and block banned words in Office 365 Word files.
545276	Phishing URIs in large PDF attachments cannot be detected.
545921	DKIM does not work properly when the email has multiple recipients.
568652	In some cases, FortiMail sends wrong URLs to FortiGuard Web Filter scan.

Mail receival and delivery

Bug ID	Description
553478	In some cases, received email is not delivered.
556364	Recipient Address Verification does not work when the internal mail server responds to SMTP connections with warning messages.
565422	SMTP connections timeout on incoming mail. FortiMail should send EOM responses after receiving all data.
530592	When both URI Click Protection and MS Office/PDF CDR are enabled, there will be milter exception error.
542901	When a large number of IBE users try to access their encrypted email simutaniously, some users may experience problems to register and access their email.

System

Bug ID	Description
561924	Nested LDAP groups deeper than two levels cannot be found.
572514	Error message when resetting an IBE user.
565860	After system reboot, IP pools fail to answer SMTP connections.
498174	LDAP alias expansion should not be case sensitive.
551045	In some cases, mailfiltered may cause high CPU usage on HA pairs.
514185	Under certain conditions, Cyrillic alphabets from some domains show incorrect encoding.
558429	Config-only HA members should not have the same entity IDs.
554636	FortiMail can be accessed from any IP address even if the IP address is different from the trusted host.
574342	After upgrading to 6.0.6 release, LDAP groups with access control policies stop working.
572983	The SNMPv3 EngineBoots parameter does not increment after system reboot.
542637	Fortinet VM appliance anti-exploit enhancement.
551408	Wrong certificate chain is supplied when the default certificate is chained and the IP pool is used.
552607	Real-only administrators cannot change their own passwords.
544856	Smtpqd memory leak.
531263	FortiMail cannot be added to the Fortinet Security Fabric anymore due to Fabric API changes.
495407	FortiMail to FortiGuard XOR encryption enhancement.

Admin GUI and webmail

Bug ID	Description
563496	Multiple attachments cannot be uploaded and sent properly in webmail.
565536	Under **Security > Quarantine > Quarantine Report > Web release host name/IP**, a port number cannot be added.
556550	Some columns of the policy table are not displayed properly.
560618	The system quarantine folder cannot be opened when the folder name contains Japanese characters.
564553	In some cases, the FotiSandbox statistics are not displayed properly under **FortiView > Threat Statistics > FortiSandbox Statistics**.
554898	Expired administrators are still displayed in the current administrator list if the administrators closed the browser without logging out from the admin GUI.
552338	The warning sign in the content disarm and reconstruction message cannot be displayed properly in Internet Explorer.
546543	The printer page opens automatically while trying to view the system quarantine page.

Log and report

Bug ID	Description
542735	Cached logs are not sent to remote log server FortiAnalyzer after FortiMail loses connection to FortiAnalyzer for a few hours.
292784	Synchronize new log fields to FortiAnalyzer.

Common vulnerabilites and exposures

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

Bug ID	Description
565946	FortiMail 6.2.0 is no longer vulnerable to the following CVE-Reference: • CVE-2019-11478 • CVE-2019-11479
565904	FortiMail 6.2.0 is no longer vulnerable to the following CVE-Reference: • CVE-2019-11477
568641	FortiMail 6.2.0 is no longer vulnerable to the following CVE-Reference: • CVE-2019-0217

Bug ID	Description
569759	FortiMail 6.2.0 is no longer vulnerable to the following CVE-Reference: • CVE-2019-12900

Known issues

The following table lists some minor known issues.

Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

(No bug ID)	TLS 1.0 support is enabled by default in 6.0 releases. After upgrading to 6.2.0 release, TLS 1.0 support will be disabled by default. Use the following CLI commands to enable TLS 1.0 support if desired:
	`config system global`
	`  set ssl-versions tls1_0 tls1_1 tls1_2`
	`end`