FortiMail - Release Notes

Version 6.0.11

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

March 25, 2021
FortiMail 6.0.11 Release Notes
06-6011-08-0707124-20210325

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-03-25	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.11 release, build 180.

Supported platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 200F
- FortiMail 400E
- FortiMail 400F
- FortiMail 900F
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000D
- 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

There are no major new features in this patch release.

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

For desktop computers:

- Microsoft Edge 88
- Firefox 77
- Safari 14
- Chrome 89

For mobile devices:

- Official Safari browser for iOS 10
- Official Google Chrome browser for Android 10, 11

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) > **6.0.11** (build 180)

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 6.0.11 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.

Antispam/Antivirus

Bug ID	Description
669438	Email classified as "TLS Session" shouldn't be counted as spam in spam reports.
667425	DOCX files uploaded into DLP sensitive data fingerprint are not detected.
666868	ISO attachments are not detected by file MIME type.
673226	DMARC check may fail for email from specific domains.
662953	Invalid URLs in email may cause email rejection.
660873	Impersonation Analysis false positives.
700919	Issues when scanning PDF files.
684937	URL click protection does not work properly with links ending with a dot.
624567	URL click protection does not properly for some email when displayed in Outlook.

Mail delivery

Bug ID	Description
663329	In some cases, FortiMail transparent mode intermittently stops passing traffic.

System

Bug ID	Description
669152	Administrator idle timeout does not work for REST API login.
663290	When email address parsing mode is set to relaxed, gateway mode also loosens LDAP recipient verification and allows non-existing hosts.

Bug ID	Description
669689	No DSNs are sent after the email in queue reaches the maximum time.
700959	Error when accessing quarantine using SSO with a proxy address not matching mail attribute.
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.
672299	The dnscached process may cache incorrect query results under heavy traffic.
608243	In some cases, LDAP authentication does not work for newly configured domains.
700244	For Diffie-Hellman key exchange, FortiMail uses self-generated parameters, which are different from the predefined finite field groups in RFC 7919.
683893	Oversized meta data is sent to FortiSandbox.
675831	The mailfilterd process causes high CPU usage.
669983	The mailfilterd process causes high CPU usage when recipient verification over SMTPS is enabled.
673811	DSN should have the hostname instead of the client IP address in EHLO.
630571	In some cases, after a secondary unit reboots in a config only HA, it cannot resynchronize with the primary unit.
656401	IP pools disappear from the access control delivery policies on config only secondary units after certain configuration changes.
658706	The mailfilterd process may exit unexpectedly while trying to decrypt archive attachments.
655958	Non-working remote FTP server for remote email archiving may cause high disk usage.
660143	In some cases, the email notification template may be reset to default.

Webmail

Bug ID	Description
662754	When sending an encrypted email, image files may not be attached in some cases.
673962	Users cannot log in to webmail with configured email aliases.
662754	When sending email with both an imbedded image and an attached image, the image attachment will not be sent.

Log and Report

Bug ID	Description
681775	Incorrect email subject encoding modifies the cross search log lines.
682102	Both accept and system quarantine actions appears in the same log.

Common vulnerabilites and exposures

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

Bug ID	Description
691547 690894 692221 692463	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').
692223	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').
693465	CWE-36: Absolute Path Traversal.
694366	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').
694751	CWE-310: Cryptographic Issues.
695037 694752	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').
695039	CWE-131: Incorrect Calculation of Buffer Size.
681403	CWE-284: Improper Access Control.

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. ***Note***: This issue has been fixed in 6.4.0 release.
594547	Due to more confining security restrictions imposed by the iOS system, email attachments included in IBE PUSH notification messages can no longer be opened properly on iOS devices running version 10 and up. Therefore, users cannot view the encrypted email messages on these iOS devices. Users should download and open the attachments on their PCs as a workaround.