



FortiMail - Release Notes

Version 7.0.1



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

September 8, 2021

FortiMail 7.0.1 Release Notes

06-701-735885-20210908

TABLE OF CONTENTS

| | |
|--|-----------|
| Change Log | 4 |
| Introduction and Supported Models | 5 |
| Supported models | 5 |
| What's New | 6 |
| What's Changed | 7 |
| Special Notices | 8 |
| TFTP firmware install | 8 |
| Monitor settings for the web UI | 8 |
| SSH connection | 8 |
| Product Integration and Support | 9 |
| FortiSandbox support | 9 |
| AV Engine | 9 |
| Recommended browsers | 9 |
| Firmware Upgrade and Downgrade | 10 |
| Upgrade path | 10 |
| Firmware downgrade | 10 |
| Resolved Issues | 11 |
| Antispam/Antivirus | 11 |
| Mail delivery | 11 |
| System | 11 |
| Log and Report | 12 |
| Admin GUI and Webmail | 12 |
| Common vulnerabilities and exposures | 13 |
| Known Issues | 14 |

Change Log

| Date | Change Description |
|------------|-------------------------------|
| 2021-09-08 | Initial release. |
| 2021-09-16 | Added a known issue. |
| 2022-04-14 | Added v7.0.0 to upgrade path. |

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 7.0.1 release, build 161.

For FortiMail documentation, see the [Fortinet Document Library](#).

Supported models

| | |
|---------------------|--|
| FortiMail | 200E, 200F, 400E, 400F, 900F, 2000E, 2000F, 3000E, 3000F, 3200E |
| FortiMail VM | <ul style="list-style-type: none">• 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 and On-Demand• Azure BYOL and On-Demand• 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 |
|---|---|
| Spam Email Submission | New Microsoft Outlook plugin for spam email submission to FortiMail. |
| Status Monitor of Backend Mail Servers | The dashboard and domain list display the status of backend mail servers. |
| Smart SMTP Recipient Verification | When the SMTP server is unreachable, store email in EC queue and deliver them after the SMTP server becomes reachable. |
| Cloud VM FIPS Support | (CLI only) New command to enable FIPS mode for VM platforms. In <code>fips-ciphers</code> mode, only a restricted set of ciphers are allowed for features requiring encryption such as SSL, TLS, and HTTPS. Other less secure protocols such as Telnet, TFTP and HTTP access to the cloud FortiMail VM are not allowed. <pre>config system fips-cc set status fips-ciphers end</pre> |
| DMARC Report | (CLI only) Support DMARC report at: <ul style="list-style-type: none">• System level (under <code>config antispam dmARC-report</code>)• Domain level (under <code>config domain</code>). |
| Authentication Enhancement | For SMTP, IMAP, POP3, and RADIUS authentication, FortiMail will try the second IP address if connection to the first IP address fails. |
| New Platform Support | Two new platforms are added: 2000F and 3000F. |
| User Account Import for Recipient Verification | (Advanced Management license required) Support for user account import in CSV format. |
| Profile Cloning | System administrator can clone system-level profiles to domain-level and then edit and use them at domain level. |

What's Changed

The following table summarizes the behavior changes in this release.

| Feature | Description |
|---------------|--|
| IP Pool Usage | IP pools can now be used for internal-to-internal email. |

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 91
- Safari 14
- Chrome 92

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) > **7.0.1** (build 161)

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 inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Antispam/Antivirus

| Bug ID | Description |
|--------|---|
| 714175 | Content profile actions are not applied correctly for Zip archives containing an *.exe file and an Office macro file. |
| 719997 | Policies with source IP filters match messages that have no client IP addresses. |
| 728397 | In some cases, FortiMail fails to allow text/plain attachments. |
| 735742 | DKIM verification may fail due to DKIM signature format reasons. |
| 740683 | SPF records using macros are flagged as SPF fail. |
| 730819 | The destination category for "s.id" URL shortening service cannot be resolved. |

Mail delivery

| Bug ID | Description |
|--------|--|
| 732505 | When DSN generation is disabled, DSNs are still sent back to the sender. |
| 700997 | Error message when sending email batches to more than 25 recipients. |
| 712202 | User-defined variables cannot be used in email templates. |

System

| Bug ID | Description |
|--------|---|
| 681597 | PDF attachment scanning may cause high CPU usage. |
| 712577 | Same as above. |
| 725014 | Same as above. |

| Bug ID | Description |
|--------|---|
| 729955 | Incorrect Japanese translation in custom messages. |
| 724386 | In config-only HA, user blocklists and safelists are not synchronized properly. |
| 720374 | Users imported from CSV files are not able to log on to FortiMail. |
| 719654 | Secondary account changes (add and delete) are not logged as system events. |
| 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. |
| 729910 | LDAP routing and recipient verification does not work properly. |
| 727609 | Updating an LDAP password that does not meets the LDAP server's password policy returns a wrong message at FortiMail webmail. |
| 728065 | High CPU due to the "expireenc" process. |
| 731620 | AWS VM license will be disabled after a few hours as duplicate by getting code 401. |
| 737770 | FortiMail to Office 365 subscription process is slow for large number of accounts. |
| 738371 | RADIUS with 2FA does not work properly. |
| 587729 | Traffic capture duration setting does not work properly. |

Log and Report

| Bug ID | Description |
|--------|---|
| 721423 | Issues with log display and log overwrite effectiveness. |
| 726648 | Log search by client location does not work properly. |
| 727678 | Domains listed in a report are not removed after the domains are deleted. |
| 733781 | Logs do not display the relay host/IP properly. |

Admin GUI and Webmail

| Bug ID | Description |
|--------|---|
| 724727 | When creating a secondary account under Domain & User > User Preference, the safelist entry is created instead. |
| 740684 | The secondary account list displays the safelist entries. |
| 724125 | The body of MIME email with non-standard HTML is not displayed in system quarantine and webmail. |

| Bug ID | Description |
|--------|---|
| 729564 | When replying to all in webmail, the sender address is also included in the recipient list. |
| 742252 | Webmail users are not able to safelist senders from the bulk folder view. |

Common vulnerabilities and exposures

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

| Bug ID | Description |
|--------|------------------------------------|
| 697129 | CWE-287: Improper authentication. |
| 690201 | CWE-20: Improper input validation. |

Known Issues

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

| Bug ID | Description |
|--------|--|
| 746912 | Email cannot be released from user quarantine or system quarantine when FortiSandbox re-scan is enabled under <i>Security > Quarantine > Quarantine Control</i> . The workaround is to disable FortiSandbox re-scan for quarantine release. |



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.