

*FortiMail™ Secure Message Platform*

*Release Notes*  
*v4.0 MR1*

06-410-112898-20100709

**FORTINET.**

## Table of Contents

<b>1 FortiMail™ v4.0 MR1 .....</b>	<b>1</b>
1.1 Summary of Enhancements.....	1
<b>2 Special Notices .....</b>	<b>2</b>
2.1 TFTP Firmware Install .....	2
2.2 Monitor Settings for Web User Interface.....	2
2.3 Web Browser Support .....	2
2.4 FortiGuard AntiSpam Service Port Change .....	2
<b>3 Firmware Upgrade/Downgrade Information .....</b>	<b>3</b>
3.1 Before and After Firmware Upgrades/Downgrades.....	3
3.2 Upgrade Path .....	3
3.3 Configuration Changes after Firmware Upgrades.....	3
3.3.1 Dictionary Settings.....	3
3.3.2 MSISDN Settings .....	4
3.4 Firmware Downgrade .....	4
3.4.1 Downgrading within v4.0 releases.....	4
3.4.2 Downgrading from v4.0 to v3.0 .....	4
<b>4 Image Checksums .....</b>	<b>5</b>

### Change Log

Date	Change Description
2010-05-28	Initial Release.
2010-07-09	GA release.

© Copyright 2010 Fortinet Inc. All rights reserved.  
Release Notes FortiMail™ v4.0 MR1.

### Trademarks

Copyright© 2010 Fortinet, Inc. All rights reserved. Fortinet®, FortiMail®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.

Support will be provided to customers who have purchased a valid support contract. All registered customers with valid support contracts may enter their support tickets via the support site:

<https://support.fortinet.com>

# 1 FortiMail™ v4.0 MR1

This document provides installation instructions, and addresses issues and caveats in FortiMail™ v4.0 MR1 Release (Build 217).

Model	FortiMail v4.0 MR1 Release Status
FML-100 FML-100C FML-400 FML-400B FML-2000 FML-2000A FML-2000B FML-4000A FML-5001A	All models are supported on the regular v4.0 MR1 branch.

## 1.1 Summary of Enhancements

The following list highlights the features added in v4.0 MR1 release. For detailed descriptions, see the FortiMail online help or the FortiMail Administration Guide.

- Identity based encryption (IBE)
- Support internal domain queries on a remote LDAP server
- Support strong-crypto for protocols such as HTTPS, SSH, SMTPS, IMAPS, and POP3S
- Add pre-defined dictionaries for DLP
- Domain-level spam report schedule is not restricted by system-level schedule settings
- Support virtual hosts for receiving inbound email
- Support iSCSI devices for mail data storage
- Bypass LDAP recipient verification if LDAP server is down
- New CLI command to back up mail queues
- User login disclaimer for admin users, webmail users, and IBE users
- Password policy enforcement for admin users, webmail users, and IBE users
- New “show full-configuration” command to display default settings which are not displayed with the “show” command
- SMTP proxy performance improvement (outbound scanning in transparent mode only)
- Support content scanning on attachment, including PDF and MS Office files
- Detection and blocking of fragmented email
- Addition of separate action to image type attachment filtering
- Treatment of SPF validation failed email as spam
- New CLI to reset default dictionary and custom messages
- Radius authentication enhancement

## 2 Special Notices

### 2.1 TFTP Firmware Install

Installing firmware during system boot time through TFTP on the serial console will erase all current FortiMail configurations and replace them with factory default settings.

### 2.2 Monitor Settings for Web User Interface

Fortinet recommends setting your monitor to a screen resolution of 1280x1024. This allows for all objects in the web UI to be viewed properly.

### 2.3 Web Browser Support

Internet Explorer 7 or higher, Firefox 3.5 or higher, and Safari 4 or higher. Adobe Flash Player 9 or higher plug-in is required to display the mail statistics charts.

### 2.4 FortiGuard AntiSpam Service Port Change

In FortiMail v3.0, queries made to the FortiGuard AntiSpam Service were accomplished using port 8889. In FortiMail v4.0, the FortiGuard AntiSpam Service port number has been made configurable and the default port has been changed to port 53. Port 8888 and 8889 are the other options.

## 3 Firmware Upgrade/Downgrade Information

### 3.1 Before and After Firmware Upgrades/Downgrades

Before any firmware upgrade/downgrade:

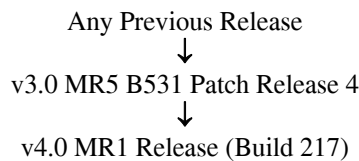
- **[FortiMail Configuration]** Save a copy of your FortiMail configuration (including replacement messages).

After any firmware upgrade/downgrade:

- **[Web UI Display]** 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.
- **[Update the AV definitions]** The AV signatures included with an image upgrade may be older than those currently available from the Fortinet's FortiGuard system. Fortinet recommends performing an immediate update as soon as possible after upgrading. Consult the FortiMail Administration Guide for detailed procedures.

### 3.2 Upgrade Path

The recommended upgrade path from previous versions is as follows:



After every upgrade, ensure that the build number and branch point match the image that was loaded.

### 3.3 Configuration Changes after Firmware Upgrades

#### 3.3.1 Dictionary Settings

In FortiMail v3.0, the dictionary settings are stored on the mail disk. In v4.0, the dictionary settings are moved to the system configuration. A sample v4.0 configuration follows:

```

config profile dictionary
  edit spamwords
    config item
      edit 1
        set pattern word1
        set pattern-scan-area header body
        set pattern-max-limit enable
        next
      edit 2
        set pattern word2
        set pattern-scan-area header body
        set pattern-max-limit enable
        next
    end
  next
end
  
```

```
config profile dictionary-group
```

```
edit dictgrp
    config dictionaries
    edit spamwords
    next
end
next
end
```

### 3.3.2 MSISDN Settings

The MSISDN settings in v3.0 under "set log msisdn enable" are not retained after upgrading to v4.0.

#### FortiMail v3.0

```
set log msisdn enable
set log msisdn-radius response enable
set log msisdn-radius secret ''
set log msisdn-radius secret-request-validate enable
set log msisdn-radius framed-ip-address network-order
```

#### FortiMail v4.0

```
config antispam settings
    set greylist-ttl 10
    set greylist-delay 20
    set bounce-verification-tagexpiry 0
    set carrier-endpoint-status enable
end
```

## 3.4 Firmware Downgrade

### 3.4.1 Downgrading within v4.0 releases

Downgrading from v4.0 MR1 to any v4.0 releases is supported.

### 3.4.2 Downgrading from v4.0 to v3.0

Direct FortiMail firmware downgrade from v4.0 to v3.0 is not supported. If you have to downgrade, all configuration and mail data will be lost.

In addition, you can only clean install the v3.0 firmware by using direct console connection. For details, see the FortiMail Administration Guide.

After you downgrade the firmware:

1. Perform "execute formatmaildisk", "execute formatlogdisk", and "execute factoryreset" to format the hard disk and reset the unit to factory defaults.
2. Configure the unit's IP address and other network settings.
3. Load back the v3.0 configuration if applicable.

## 4 Image Checksums

The MD5 checksums for the firmware images are available at the Fortinet Customer Support website (<https://support.fortinet.com>). After logging in, click on the "Firmware Images Checksum Code" link in the left frame.

(End of Release Notes.)