

## **Upgrade Guide for FortiMail 3.0**

After this guide is initially released, it is published periodically to update information or correct errata concerning the current firmware version. Fortinet recommends reviewing the current version of this guide, since it contains revised and updated information.

A current version of the Upgrade Guide for FortiMail 3.0 is located at <http://docs.forticare.com>.

**FORTINET™**

[www.fortinet.com](http://www.fortinet.com)

*Upgrade Guide for FortiMail 3.0*

Version 3.0 MR2

10 December 2007

06-30002-0422-20071210

© Copyright 2007 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

### **Trademarks**

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

### **Regulatory compliance**

FCC Class A Part 15 CSA/CUS

# Contents

<b>Introduction .....</b>	<b>7</b>
<b>About this document.....</b>	<b>7</b>
Document conventions.....	7
Typographic conventions.....	8
<b>FortiMail documentation .....</b>	<b>8</b>
Fortinet Tools and Documentation CD.....	9
Fortinet Knowledge Center .....	9
Comments on Fortinet technical documentation.....	9
<b>Customer service and technical support .....</b>	<b>9</b>
<b>3.0 MR2 features and changes.....</b>	<b>11</b>
<b>Overview of the new features and changes .....</b>	<b>11</b>
<b>New features and changes .....</b>	<b>12</b>
Administrators in FortiMail 3.0 MR2 .....	12
Quick Start Wizard .....	13
Basic management mode .....	13
Management.....	14
Settings.....	15
Log & Report.....	15
Advanced management mode .....	15
Mail Settings.....	15
Mail queue default settings .....	15
Failed Queue .....	16
Policy.....	16
IP Policy changes .....	16
Policy options.....	16
Log & Report.....	17
Predefined reports .....	17
Re-ordering of log type tabs .....	18
Status page includes History logs.....	18
High Availability (HA) .....	18
<b>3.0 MR1 features and changes.....</b>	<b>21</b>
<b>Overview of new features and changes .....</b>	<b>21</b>
<b>New features and changes .....</b>	<b>22</b>
Anti-Spam .....	22
PDF scan option .....	22
Deep header scanning.....	22
Dynamic heuristic rules using the FortiGuard-Antispam service .....	23
Regular expression behavior .....	23

<b>3.0 features and changes .....</b>	<b>25</b>
<b>Overview of new features and changes .....</b>	<b>25</b>
<b>New features and changes .....</b>	<b>27</b>
Email header information .....	27
Real-time Blackhole List (RBL) renamed to DNS Block List (DNSBL) .....	27
System .....	27
Mail Settings .....	27
Domain configuration.....	27
Relay server .....	27
Spam, Anti-Virus and content filtering custom messages .....	28
Spam and summary email report custom formats.....	28
User .....	28
Profile.....	29
Multiple spam actions.....	29
Regex .....	29
Multiple language .....	29
Scanning images in emails.....	29
Policy .....	29
Anti-Spam .....	30
Bayesian filtering .....	30
Auto-training Bayesian databases.....	30
Training using mbox files.....	31
Training using control accounts.....	31
Maintaining Bayesian databases.....	31
Black/white lists (system, session and personal) .....	31
Greylist .....	32
System Quarantine.....	32
Log & Report.....	32
High Availability (HA) .....	33
Webmail .....	33
<b>Managing firmware versions .....</b>	<b>35</b>
<b>FortiMail 3.0 upgrade information.....</b>	<b>35</b>
Loading default profiles.....	35
Configuration limits .....	36
Heuristic default setting changes (3.0 MR1) .....	36
IP-based policy changes (3.0 MR2).....	37
Resetting to factory defaults in FortiMail 3.0 MR2 .....	37
<b>Backing up your configuration .....</b>	<b>37</b>
Backing up your configuration using the web-based manager .....	37
Backing up your configuration using the CLI .....	38
<b>Upgrading your FortiMail unit .....</b>	<b>38</b>
Upgrading to a current firmware version.....	38
Verifying the upgrade.....	40

<b>Reverting to a previous firmware version .....</b>	<b>40</b>
Downgrading to a previous firmware version .....	41
Reconnecting to the FortiMail unit.....	42
Restoring the previous configuration.....	43
<b>Index.....</b>	<b>45</b>



# Introduction

Over the past year, Fortinet has been developing, testing and refining a new operating system for your FortiMail unit. FortiMail 3.0 is a more dynamic and robust operating system, offering you even better protection, blocking and monitoring features for email on your network.

This guide provides you with information on FortiMail 3.0, and addresses any issues that may arise concerning your current configuration. With these new features, and improvements to existing features, you need to know how they may or may not affect your current configuration. This guide provides you with information on backing up your current configuration, and installing FortiMail 3.0 on your FortiGate unit.

FortiMail 3.0 firmware release information is also included in this guide.

## About this document

This document contains the following chapters:

- [3.0 MR2 features and changes](#) – Provides information about new features as well as changes to existing features for FortiMail 3.0 MR2.
- [3.0 MR1 features and changes](#) – Provides information about three new features as well as changes to heuristic rules and regular expression behavior for FortiMail 3.0 MR1.
- [3.0 features and changes](#) – Provides information about new features and changes for FortiMail 3.0.
- [Managing firmware versions](#) – Describes how to install FortiMail 3.0 and revert back to FortiMail 2.8. Includes issues about FortiMail 3.0, how to back up current configuration settings, re-establish connections after the upgrade, and verify that the upgrade is successfully installed.

## Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:



**Note:** Highlights useful additional information.



**Caution:** Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

## Typographic conventions

FortiMail documentation uses the following typographical conventions:

Convention	Example
<b>Keyboard input</b>	To navigate the list of sessions, select the Page Up icon or the Page Down icon.
<b>CLI command syntax</b>	<code>execute restore config &lt;filename_str&gt;</code>
<b>Document names</b>	<i>FortiMail Administration Guide</i>
<b>Menu commands</b>	Go to <b>System &gt; Network &gt; Interface</b> to view the interface information.
<b>Program output</b>	Welcome!
<b>Variables</b>	<address_ipv4>

## FortiMail documentation

Information about the FortiMail unit is available from the following guides:

- *FortiMail QuickStart Guides*  
Provides basic information about connecting and installing a FortiMail unit. A separate guide is available for each FortiMail model.
- *FortiMail Administration Guide*  
Introduces the product and describes how to configure and manage a FortiMail unit, including how to create profiles and policies, configure antispam and antivirus filters, create user accounts, configure email archiving, and set up logging and reporting.
- *FortiMail CLI Reference*  
Describes how to use the FortiMail CLI and contains a reference of all FortiMail CLI commands.
- *FortiMail Log Message Reference*  
Available exclusively from the [Fortinet Knowledge Center](#), the *FortiMail Log Message Reference* describes the structure of FortiMail log messages and provides information about the log messages that are generated by FortiMail units.
- *FortiMail Installation Guide*  
Describes how to set up the FortiMail unit in transparent, gateway, or server mode.
- *FortiMail online help*  
Provides a searchable version of the *FortiMail Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Webmail online help*  
Describes how to use the FortiMail web-based email client, including how to send and receive email, how to add, import, and export addresses, how to configure message display preferences, and how to manage quarantined email.

- *FortiMail User Guides*

Provides information that the FortiMail end users need to know in order to take advantage of the services provided by the FortiMail unit. These guides are included as chapters in the *FortiMail Administration Guide*, allowing the administrator to provide information on only the enabled features.

## Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

## Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

## Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

# Customer service and technical support

Fortinet Technical Support provides services designed to make sure your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services Fortinet provides.



# 3.0 MR2 features and changes

FortiMail 3.0 MR2 contains the new basic management mode, a quick start wizard, as well as changes to existing features. The current web-based manager is now called advanced management mode. It is recommended that current administrators become familiar with the basic management mode because it is the default mode after resetting the FortiMail unit to factory defaults.

After successfully upgrading to FortiMail 3.0 MR2, current administrators log into the familiar web-based manager now called the advanced management mode.

These new features for FortiMail 3.0 MR2 do not conflict with current configuration settings.

This section contains the following topics:

- [Overview of the new features and changes](#)
- [New features and changes](#)

Fortinet recommends reading the following documents for any additional information about the new features and changes in FortiMail 3.0 MR2.

- *FortiMail Administration Guide*
- *FortiMail CLI Reference*



**Note:** Configuration of settings in the following menus are unchanged unless otherwise stated. See [“Managing firmware versions” on page 35](#) for information about upgrading to FortiMail 3.0 MR2.

The CLI interface does not differentiate between modes.

## Overview of the new features and changes

New features and changes for FortiMail 3.0 MR2 are:

- **Quick Start Wizard** – The quick start wizard provides an easy, step-by-step process for configuring the required information to get the FortiMail unit up and running. See [“Quick Start Wizard” on page 13](#) for more information.
- **Basic management mode** – In basic management mode, there are only basic features, providing an introduction to FortiMail features for beginning FortiMail administrators. This mode is also useful to quickly set up basic settings for advanced FortiMail administrators. See [“Basic management mode” on page 13](#) for more information.
- **Advanced management mode** – In advanced management mode, all features and configuration settings are available. See [“Advanced management mode” on page 15](#) for more information.
- **Mail queue default setting changes** – Mail queue default settings changed. The Failed Queue tab is no longer available. Failed emails now display in the Dead Mail Queue tab. See [“Mail Settings” on page 15](#) for more information.

- **IP-based policy changes** – IP-based policies are no longer used for both POP3 and Webmail access; recipient-based policies are used instead. See [“IP Policy changes” on page 16](#) for more information.
- **Logging menu enhancement** – The log type tabs display in a different order. See [“Log & Report” on page 17](#) for more information.
- **System Status page displays History logs** – History logs now display from the Status page. See [“Log & Report” on page 17](#) for more information.
- **High Availability recovery mode options** – There are two new recovery options available for configuring what the FortiMail unit does when a failure occurs. You can also now configure up to 24 subordinate units in a high availability cluster. See [“High Availability \(HA\)” on page 18](#) for more information.

## New features and changes

The following descriptions include only menus containing new features, changes to existing features, or both. Procedural information is included where applicable.

### Administrators in FortiMail 3.0 MR2

The Admin tab has a new setting for administrators, Management mode, that enables administrative access to either basic management mode or advanced management mode. These modes are available for both current and new administrators.

**Figure 1: Administrative settings in FortiMail 3.0 MR2**

The screenshot shows a 'New Administrator' configuration dialog box. It includes the following fields and options:

- Administrator:** A text input field.
- Domain:** A dropdown menu with 'system' selected.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Trusted Host:** A text input field containing '0.0.0.0'.
- Netmask:** A text input field containing '0.0.0.0'.
- Permission:** Three radio buttons: 'Read Only' (selected), 'Read & Write', and 'Administrator'.
- Management mode:** Two radio buttons: 'Basic' (selected) and 'Advanced'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

By default, current administrator access settings are set to advanced management mode and newly created administrators are set to basic management mode.

You can configure administrative access to either basic or advanced management mode in **System > Config > Admin** (in advanced management mode) or **Settings > Config > Admin** (in basic management mode). Administrators who want to change administrative access settings can do so while in either basic management mode or advanced management mode.

## Quick Start Wizard

The quick start wizard helps you to customize basic configuration settings for your FortiMail unit. The quick start wizard displays after selecting the Quick Start menu.

After selecting the Quick Start menu, you are directed through a series of steps. In each step you enter the appropriate information. For example, in Step 1 you enter your own password and confirm this password. If you skip a step or enter wrong information, a notification appears.

**Figure 2: Configuring system settings in Step 2 of the Quick Start Wizard**

The quick start wizard provides the beginning FortiMail administrator a way to quickly have the FortiMail unit up and running quickly. An advanced FortiMail administrator can also use the quick start wizard to quickly configure basic settings after the FortiMail unit has been reset to factory defaults.

## Basic management mode

The basic management mode is for the beginning FortiMail administrator; however, this mode is also useful to the advanced FortiMail administrator. In basic management mode, an advanced FortiMail administrator can easily and quickly configure basic settings, including mail settings, and also view logs and reports.

Accessing either the basic management mode or the advanced management mode is determined by the Management mode setting for each administrator. See [“Administrators in FortiMail 3.0 MR2” on page 12](#) for more information.

**Figure 3: Basic management mode in the web-based manager**

The menus available in basic management mode are:

- Management – includes the Status, Mail Queue and Quarantine menus
- Settings – includes the Config, Network, Domains, and AntiSpam menus
- Log & Report – includes the Logging, Report and Alert Email menus

The basic management mode also includes the quick start wizard and the Advanced menu. The Advanced menu enables you to switch from basic management mode to advanced management mode at any time.

The following procedure describes how to switch from basic to advanced management mode. This procedure assumes that you are already in basic management mode.

#### To switch to advanced management mode

- 1 In basic management mode, select Advanced.

The following question appears:

Are you sure you want to switch to advanced management mode?

- 2 Select OK.

You are redirected to advanced management mode in the web-based manager.

## Management

The Management menu contains three menus: Status, Mail Queue and Quarantine. The Status menu contains two tabs, the Status tab and the Mail Statistics tab. These two tabs are the same as in previous firmware versions. The Mail Queue menu contains the tabs Deferred Queue, Spam Queue, Dead Mail, and Queue Maintenance.

The Quarantine menu contains the Recipients tab and System quarantine tab.

## Settings

The Settings menu contains the Config, Network, Domains, and AntiSpam menus.

The Config menu contains the Time and Admin tabs. The Network menu contains the Interface, DNS and Routing tabs. The Domains menu contains the Domains and Local Host tabs. The AntiSpam menu contains the Incoming, Incoming Action, Outgoing, and Outgoing Action tabs.

## Log & Report

The Log & Report menu contains the Logging, Reports and Alert Email menus. The Logging menu contains the four log type tabs: History, Event, AntiSpam and AntiVirus. These tabs were re-arranged for FortiOS 3.0 MR2. The Alert Email menu contains the Categories and Alert Email tabs.

## Advanced management mode

The advanced management mode is for the advanced FortiMail administrator or a FortiMail administrator familiar with the new basic management mode, and is ready for more advanced features. Current administrators logging into the web-based manager default to advanced management mode.

The previous web-based manager is now called the advanced management mode and contains all the features current administrators are familiar with.

The following procedure describes how to switch from advanced management mode to basic management mode. This procedure assumes that you are already in advanced management mode.

### To switch to basic management mode

- 1 In advanced management mode, select Basic.

The following question appears:

Are you sure you want to switch to basic management mode?

- 2 Select OK.

You are redirected to the basic management mode in the web-based manager.

## Mail Settings

The Mail Settings menu contains changes to the mail queue default settings in both management modes. The Failed Queue tab is no longer available from the Advanced menu, in both management modes.

### Mail queue default settings

The default settings for Mail Queue changed for FortiMail 3.0 MR2. These settings will not affect Mail Queue settings that carry forward.

**Figure 4: Default Mail Queue settings**

<b>Mail Queue</b>	
Maximum time for email in queue (1-10 days):	<input type="text" value="5"/>
Maximum time for DSN email in queue (0-10 days):	<input type="text" value="5"/>
Time before delay warning (1-24 hours):	<input type="text" value="4"/>
Time interval for retry (10-120 minutes):	<input type="text" value="27"/>

The following table outlines what each parameter contains in FortiMail 3.0 MR2:

<b>Maximum time for email in queue (1-10 days):</b>	The default is now 5 days. Enter a number between 1 and 10 to configure the maximum time out before a message is returned as undeliverable.
<b>Maximum time for DSN email in queue (0-10 days):</b>	The default is now is 5 days. Enter a number between 0 and 10 to configure the maximum time out before a message is returned as undeliverable for delivery status notification messages. The value 0 means that the DSN email is tried only once and is not retained in the queue if the email is undeliverable.
<b>Time before delay warning (1-24 hours):</b>	The default is now 4 hours. Enter a number between 1 and 24 to configure the time out before a warning message is sent to the sender informing the sender that the message is now deferred.
<b>Time interval for retry (10-120 minutes):</b>	The default is now 27 minutes. Enter a number between 10 and 120 to configure the minimum amount of time an email must sit in the queue between queue runs. This option sets the queue to run at a low interval for better responsiveness without trying all emails in each run.

## Failed Queue

The Failed Queue tab was removed for FortiMail 3.0 MR2. Emails that displayed in the Failed Queue tab are now found in **Mail Settings > Mail Queue > Dead Mail** (in advanced management mode) or **Management > Mail Queue > Dead Mail** (in basic management mode).

## Policy

The Policy menu contains changes for IP-based policies as well as the removal of options in **Policy > IP Based > IP Policies**. These changes affect both management modes.

### IP Policy changes

Previously, authentication for POP3 and WebMail access went through an IP-based policy first; now, recipient-based policies are used first for POP3 and Webmail access.

This change occurred because of issues that occur with authentication for POP3 and WebMail access as well as IP-based policies can also match outgoing emails.

### Policy options

In **Policy > IP Based > IP Polices**, the options Allow POP3 for SPAM access and Allow Web Mail for SPAM access are no longer available.

Figure 5: Configuration settings for IP policies

## Log & Report

The Log & Report menu contains changes to the order of tabs in the Logging menu, including History logs displaying on the Status page, and two default predefined reports.

### Predefined reports

FortiMail 3.0 MR2 includes two default predefined reports in the Report menu, called `predefined_report_yesterday` and `predefined_report_last_week`. The predefined reports are automatically configured after using the quick start wizard to configure basic settings.

The predefined report, `predefined_report_yesterday`, collects all logs recorded by the FortiGate unit on the previous day. For example, if the `predefined_report_yesterday` was created on November 3, then the logs recorded on November 2 would be used in that report. In a similar way, the `predefined_report_last_week` collects all logs recorded by the FortiGate unit for the past week. For example, if the `predefined_report_last_week` was created on November 15, logs recorded in the previous week would be used in that report.

Each pre-defined report comes with the same default settings, except for the queries: `predefined_report_last_week` contains an extra query, High Level Breakdown. These reports have no schedule so you need to manually generate them from the Config page. See the *FortiGate Administration Guide* for more information about configuring reports.

The following table shows the default settings for the predefined reports that are available in **Log & Report > Reports > Config**:

<b>Report Name</b>	Either <code>predefined_report_yesterday</code> or <code>predefined_report_last_week</code> .
<b>Time Period</b>	Either Yesterday or Last Week is selected from the drop-down list.
<b>Queries</b>	The queries are Mail Statistics and Total Summary for <code>predefined_report_yesterday</code> , with the High Level Breakdown also available with <code>predefined_report_last_week</code> .

<b>Schedule</b>	Not Scheduled is selected.
<b>Domain</b>	All Domains is selected.
<b>Incoming Outgoing</b>	Incoming and Outgoing is selected.
<b>Output</b>	PDF report is selected but no email addresses are configured for sending the report to others.



**Note:** Predefined reports are available only if you configure basic settings using the quick start wizard. These reports are configured using the information entered for basic settings in the quick start wizard.

## Re-ordering of log type tabs

In the Logging menu, the tabs are re-arranged in the following order:

- History
- Event
- AntiVirus
- AntiSpam

## Status page includes History logs

The System Status page now includes History logs, located in History Logs. This is available in both advanced management mode and basic management mode. This replaces the previous History resources display. The History logs that display on the System Status page contain navigational features as well as allowing you to download, empty and delete log files.

History logs contain all log messages that are recorded by the FortiMail unit.

## High Availability (HA)

FortiMail 3.0 MR2 includes a new mode for High Availability (HA), available in advanced management mode. The new HA Recovery mode detects a recovery and moves the FortiMail device into either subordinate or primary unit mode. You can also now configure up to 24 subordinate units in a HA cluster, also available in advanced management mode.

The previous mode entered an OFF state. In this state, the FortiMail unit required manual intervention before it could return to its original role in the HA cluster.

The new options are available in **System > HA > Configuration**. You can select these options in the Main Configuration section of the HA Configuration page. These new options are:

- switch OFF – The previous mode for HA recovery. This switches the FortiMail unit offline from the HA cluster; the FortiMail unit must then be manually brought back online from the web-based manager.
- wait for recovery then restore original role – The FortiMail unit resumes the original mode of operation. For example, if the FortiMail unit was a primary unit before the failure occurred, it resumes being a primary unit after recovering from the failure.
- wait for recovery then restore assume slave role – This mode enables the FortiMail unit to take on the subordinate mode role after a failure occurs.

It is recommended to select the option, "wait for recovery then assume slave role" because it is useful in most configurations. Synchronization issues may arise for certain configurations if the option, "wait for recovery then restore original role", is selected.



# 3.0 MR1 features and changes

FortiMail 3.0 MR1 provides three new features for anti-spam: PDF scanning, deep header scanning, and dynamic heuristic rules. Changes occurred for both heuristic rules and regular expression behavior.

This section contains the following topics:

- [Overview of new features and changes](#)
- [New features and changes](#)

Fortinet recommends reading the following documents for any additional information about the new features and changes in FortiMail 3.0 MR1.

- *FortiMail Administration Guide*
- *FortiMail CLI Reference*



**Note:** Configuration of settings in the following menus are unchanged unless otherwise stated. See [“Managing firmware versions” on page 35](#) for information about upgrading to FortiMail 3.0MR1.

## Overview of new features and changes

New features and changes for FortiMail 3.0 MR1 are:

- **PDF scan option** – The PDF scan option can scancheck the first page of PDF attachments for spam by the heuristic, banned word and image spam scanners. See [“PDF scan option” on page 22](#) for more information.
- **Deep header scanning** – Deep header scanning looks at all email headers and performs a decision tree analysis on the available information. See [“Deep header scanning” on page 22](#) for more information.
- **Dynamic heuristic rules using the FortiGuard Anti-spam service** – Dynamic heuristic rules replace statistic heuristic rules. Default settings for both upper and lower threshold values changed as well. See [“Dynamic heuristic rules using the FortiGuard-Antispam service” on page 23](#) for more information.
- **Regular expression behavior** – Regular expression behavior, as defined in the Dictionary profile, has changed. See [“Regular expression behavior” on page 23](#) for more information.

## New features and changes

The following descriptions include only menus containing new features, changes to features, or both. Procedural information is included where applicable.

### Anti-Spam

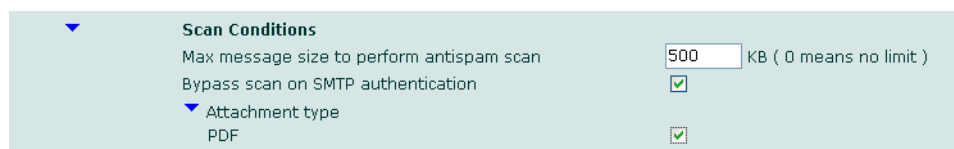
The Antispam menu is the only menu in FortiMail 3.0 MR1 that has new features and changes.

#### PDF scan option

The PDF scan option provides a way to scan PDF attachments. The PDF scan option is enabled in **Profile > Anti-Spam**, in the Scan Conditions section of the Anti-spam Profile page.

When this option is enabled, the heuristic, banned word, and image spam scan examines the first page of each PDF attachment to determine if the message is spam. At least one of these three related scanning methods must be enabled for PDF scanning to work.

**Figure 6: PDF scan enabled in an antispam profile**



If any of the content in any of the PDF attachments triggers any rule, a log message records entries such as the following:

```
2007-10-29 16:36:57 log_id=0501080300 type=spam
subtype=detected pri=information session_id="l9TKaiTm001036"
client_name="[192.168.110.35]" from="aabb@xyncompany.com"
to="ccdd@xyncompany.com" subject="[tp] [SPAM detected by
FortiMail] headquarters" msg="Rejected by BannedWord cytv
Found banned words in a PDF attachment"
```

The message field may also contain the following:

```
"Rejected by Heuristic check. Score <score_value> there were
rules triggered by PDF text"
```

#### Deep header scanning

Deep header scanning includes two scan options, black IP scan and deep header analysis. Deep header scanning is enabled in **Profile > Anti-Spam**, in the Deep header scan section of the Anti-spam Profile page.

**Figure 7: Deep header scanning and options in an anti-spam profile**



A Black IP scan looks at the “Received” field of the email headers. IP addresses are extracted from the headers and results are passed to the configured DNSBL servers. IP addresses are also checked against the FortiGuard-Antispam black list, if deep header scan, black IP scan, and FortiGuard-Antispam Black IP scan are enabled. The Black IP option of FortiGuard-Antispam must also be enabled for FortiGuard-Antispam to check every address in the received lines. If deep header scanning is disabled, only SMTP client IP is checked against the FortiGuard-Antispam black list.

Deep header analysis looks at all of the email headers and performs a decision tree analysis from available information. Deep header analysis configuration includes Confidence degree, Trusted Server IP and Trusted IP list. The “Received” header that contains the IP address in the Trusted IP list is not checked. The “Received” headers listed after the Received header, which contains IP addresses included in the Trusted Service IP list, are also not checked.

If deep header analysis and deep header scan are both enabled, deep header analysis performs a decision tree analysis after Image Spam scanning is performed.

## Dynamic heuristic rules using the FortiGuard-Antispam service

FortiMail 3.0 MR1 replaces statistic heuristic rules with dynamic heuristic rules. Default heuristic rules changed as well.

Heuristic rules are no longer accessible for administrators in **Anti-Spam > Rules**.

The heuristic scan option now includes three parameters: lower threshold, upper threshold, and the percentage of rules used.

The Dynamic heuristic rules feature includes changes to the default settings for both upper and lower threshold values. The default threshold values are now -20.000/3.500. You need to review your settings for heuristic rules after upgrading, starting with the default thresholds. You can enable and configure threshold settings for heuristic rules in **Profile > Anti-Spam**, in the Heuristic scan section of the Anti-spam Profile page.

**Figure 8: Configured heuristic rules and percentage of rules used**

<input type="checkbox"/>	▼	<b>Heuristic scan</b>	Actions	Default
		Lower level threshold		-20.000
		Upper level threshold		3.500
		The percentage of rules used		25

## Regular expression behavior

Previously in **Profile > Dictionary**, if the pattern began with a number or a letter, the pattern was treated as if a \b prefix was added; also, if a pattern ended with a letter or number, then \b is added to the end. This could occur for both. For example, the pattern `write` was recognized as `\bwrite\b` because it began with a lower-case w.

In FortiMail 3.0 MR1, regular expression behavior is changed so that the prefix `\b` is not added to a pattern when beginning with a letter or number, or ending with a letter or number. This provides better matches when searching for specific patterns. For example, the pattern `write` is now recognized as `write`, and words such as `rite` or `ite` will also match.

# 3.0 features and changes

FortiMail 3.0 provides several new features and changes to existing features, including a global Bayesian database, aggressive image scanning, support for a second FortiAnalyzer unit or Syslog server, and DDNS enhancements.

This section contains the following topics:

- [Overview of new features and changes](#)
- [New features and changes](#)

Fortinet recommends reading the following documents for any additional information about the new features and changes in FortiMail 3.0.

- *FortiMail Administration Guide*
- *FortiMail CLI Reference*

You may also want to review these documents that are available at the Fortinet Knowledge Center:

- FortiMail Best Practices
- FortiMail 3.0 Maximum Values Matrix



**Note:** Configuration of settings in the following menus are unchanged unless otherwise stated. See [“Managing firmware versions” on page 35](#) for information about upgrading to FortiMail 3.0.

The issue concerning software Raid on the FortiMail-400 unit is now resolved.

## Overview of new features and changes

New features and changes for FortiMail 3.0 are:

- **Email header information** – The email header information now includes the word that triggered both dictionary and banned word filters. See [“Email header information” on page 27](#) for more information.
- **Real-time Blackhole List (RBL) name change** – DNS Block List replaces RBL. See [“Real-time Blackhole List \(RBL\) renamed to DNS Block List \(DNSBL\)” on page 27](#) for more information.
- **Bayesian filtering** – FortiMail 3.0 now includes auto-training, training with mbox files, using control accounts, and maintaining Bayesian databases. See [“Bayesian filtering” on page 30](#) for more information.
- **Black/white lists** – White lists are now checked before black lists, enabling the white listing specific addresses within a black listed domain. See [“Black/white lists \(system, session and personal\)” on page 31](#) for more information.
- **Greylist checking** – You can now set the greylist initial expiry period from 4 to 24 hours, and modify the maximum number of greylist entries. See [“Greylist” on page 32](#) for more information.

- **Scanning images in emails**– An aggressive scanning option is now available for scanning images in emails, providing specific scanning of images within email messages. See [“Scanning images in emails” on page 29](#) for more information.
- **Quarantine administrator support** – The quarantine administrator can now log in to the web-based manager interface and view all system quarantine messages. See [“System Quarantine” on page 32](#) for more information.
- **Multiple spam actions per profile** – You can now configure multiple spam actions per profile in FortiMail 3.0. See [“Profile” on page 29](#) for more information.
- **Multiple language support** – The dictionary now supports multiple languages, including double-byte character sets. See [“Profile” on page 29](#) for more information.
- **Regex support** – The dictionary now supports Regex for text patterns. See [“Profile” on page 29](#) for more information.
- **Editing profiles**– You can now edit a profile from within a policy page, providing improved usability. See [“Policy” on page 29](#) for more information.
- **Email alias** – You can now define an email alias as a member when configuring email aliases. See [“User” on page 28](#) for more information.
- **Domain configuration** – When configuring domains, the FortiMail local domain is now the same as one of the defined mail server domains. This means that companies and organizations require only a second hostname and not an entirely new domain. See [“Domain configuration” on page 27](#) for more information.
- **Relay servers** – Relay servers now support SMTP authentication. See [“Relay server” on page 27](#) for more information.
- **Spam, Anti-Virus and content filtering custom messages** – Custom messages for spam, Anti-Virus and content filtering can now be reset to default settings. See [“Spam, Anti-Virus and content filtering custom messages” on page 28](#) for more information.
- **Spam and summary email report custom formats** – You can now customized spam and summary email report formats. See [“Spam and summary email report custom formats” on page 28](#) for more information.
- **Dynamic DNS (DDNS)** – FortiMail 3.0 has added several features and options that include custom domains, auto-detect IP mode, TLS, and SMTP authentication. See [“System” on page 27](#) for more information.
- **Multiple FortiAnalyzer units and Syslog servers support** – You can now configure the FortiMail unit to log to multiple FortiAnalyzer units or Syslog servers. See [“Log & Report” on page 32](#) for more information.
- **Log messages include word trigger** – Log messages in FortiMail 3.0 now include the word that triggered the banned word check or dictionary check. See [“Log & Report” on page 32](#) for more information.
- **Network interface configuration for High Availability (HA)** – A FortiMail network interface does not support both user data and HA synchronization. See [“High Availability \(HA\)” on page 33](#) for more information.
- **Webmail interface changes** – You can customize the webmail login banner to display, for example, the company or organization’s name. You can also configure Webmail so that users automatically connect to HTTPS Webmail. See [“Webmail” on page 33](#) for more information.

## New features and changes

The following descriptions include only menus containing new features, changes to existing features, or both. Procedural information is included where applicable.

### Email header information

The email header information now includes the word that triggered the dictionary and banned word filters. The email header information can help determine which methods are effective or the methods that may be causing false positives.

### Real-time Blackhole List (RBL) renamed to DNS Block List (DNSBL)

In FortiMail 3.0, RBL is now DNSBL. Both the web-based manager and CLI reflect this name change. DNSBL is still part of the FortiGuard Anti-Spam service and is considered a “living” list of known spam origins.

### System

FortiMail 3.0 includes additional features and options for DDNS. These new features and changes include custom domains, auto-detect IP mode, TLS and SMTP authentication.

Auto-detect IP mode is available only in the CLI. TLS and SMTP authentication are also available only in the CLI, and are configured using the `set auth smtp server` command syntax. Auto-detect IP mode, TLS and SMTP authentication apply to all domains.

You can now configure a proxy server that uses the HTTPS proxy for secure Anti-virus and IPS updates. HTTPS proxy support is now available for antivirus updates and is available only from the CLI.

### Mail Settings

The Mail Settings menu contains changes to configuring domains, reverting to default settings within custom messages, and SMTP authentication for relay servers.

#### Domain configuration

The FortiMail local domain is now the same as one of the defined mail server domains. The change means that companies or organizations that do not have a second domain or the ability to manage their own domains only need a second hostname for the FortiMail unit and do not need to add an entirely new domain. This type of configuration eliminates confusion that may come about from using a different email domain for the FortiMail unit.

This type of domain configuration also requires other configuration changes to properly work. For example, email is redirected from the Bayesian control accounts to the FortiMail unit by using aliases or hiding the mail server behind the FortiMail unit so that the FortiMail unit intercepts the special emails.

#### Relay server

SMTP authentication support for relay servers is now available in **Mail Settings > Settings**. When configuring a relay server, you can also include authentication for the SMTP user.

## Spam, Anti-Virus and content filtering custom messages

You can now reset current custom messages to default options for each spam, Anti-Virus and content filtering message in **Mail Settings > Settings > Custom Messages**.

You can revert current custom messages back to default messages within each custom message by selecting the Reset to Default link. This link appears in each custom message in the Custom Messages page.

**Figure 9: Reset to Default link in the Content filtering custom message window**



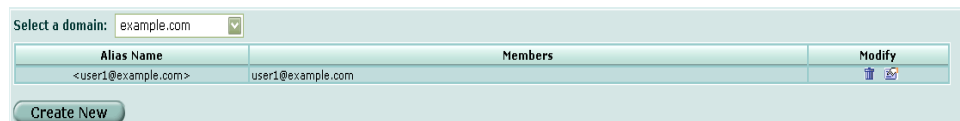
## Spam and summary email report custom formats

You can now customize the spam and summary report in **Mail Settings > Settings > Custom Messages**. The reports can also be reset to default settings by selecting Reset to Default. The Release All link is no longer supported.

## User

An email alias can define itself as a member in **User > User Alias**.

**Figure 10: An email alias as a member**



## Profile

The Profile menu contains several new features and changes. FortiMail 3.0 supports multiple spam actions, Regex for text patterns, and multiple languages in the dictionary.

### Multiple spam actions

Profiles now support multiple spam actions per spam profile. You can now define different actions for each spam detection method within a spam profile, providing more flexibility for handling spam.

### Regex

Regular Expressions (Regex) for text patterns is supported in the dictionary. You can use Regex to create dictionary profiles to block confidential message content, such as credit card numbers, telephone numbers, SSN/SIN numbers, and internal email addresses. For example, `SSN: \d{3}-\d{2}-\d{4}`.

### Multiple language

Multiple languages are supported in the dictionary, including double-byte character sets. The FortiMail dictionary performs as follows:

- FortiMail saves the dictionary in UTF-8 format
- incoming email is converted to UTF-8 format according to the MIME type of the email
- FortiMail tries to match the pattern

For example, if the MIME header of the email has `charset="iso-2022-jp"`, FortiMail converts the email to UTF-8 before performing the pattern matching. This means the dictionary analysis will work with any language or character set. Double-byte character expressions can be cut and pasted in the FortiMail web-based manager. FortiMail converts the characters to UTF-8.

### Scanning images in emails

In **Profile > Anti-Spam**, you can now choose to aggressively scan images within emails. This aggressive scanning option enables the FortiMail unit to be more critical in determining what email messages contain spam.

In the Anti-Spam profile, you can enable the Aggressive scan option after expanding the Image spam scan section so that the FortiMail unit examines image file attachments in addition to embedded images.

Aggressive scanning could affect performance with traffic containing images files.

## Policy

You can now edit a profile from either **Policy > Recipient Based** or from **Policy > IP Based**. There are links to each profile that are associated with the policy that was created in the Policy menu. For example, you are viewing recipient policies and notice you need to change the anti-spam profile; you select the anti-spam profile link on the Incoming by selecting the profile, that profile's page appears and you then proceed to change and save the profile.

**Figure 11: Links for each profile from Incoming Recipient Policies**

#	User Name	Anti-spam Profile	AV Profile	Content Profile	Auth Profile
1	*	<a href="#">antis spam_def</a>	<a href="#">antivirus_def</a>	<a href="#">content_def</a>	<a href="#">(none)/(none)</a>

## Anti-Spam

The Anti-Spam menu contains new features and changes for Bayesian, Black/White lists, Greylists and System quarantine.

### Bayesian filtering

Bayesian filtering supports outbound email policies along with a new top level Bayesian database called the Global Bayesian database for the FortiMail unit. You can now use a single Global Bayesian database for all domains, resulting in a more maintainable database, or define a group and user level database for more granularity. There are now three Bayesian databases:

- Global (system level)
- Group (domain level)
- User (individual user databases)

The Global Bayesian database applies to all users in all domains. A Bayesian database is not mature until it is trained with 100 spam emails and 200 non-spam (clean) emails.



**Note:** Bayesian filtering should be used with caution since it requires an advanced understanding of Bayesian database training.

A sample Bayesian database is not provided in FortiMail 3.0 because of the differences in spam trends across geographical regions. Auto-training a Bayesian database develops a mature database quickly and does not require a sample database.

### Auto-training Bayesian databases

You can automatically train a Bayesian database if “Use other techniques for auto training” is enabled as part of the antispam profile in an active policy. The FortiMail unit can train the database with results from the FortiGuard-AntiSpam filter (learn is spam), SURBL filter (learn is spam), system white list (learn is not spam), and user white list (learn is not spam).

Bayesian database training depends on the FortiMail configuration. Auto-training a Bayesian database stops after the database counts reach 100 spam emails and 200 clean emails. If the database does not have 100 spam emails and 200 clean emails, the database is trained by results from the FortiGuard-AntiSpam filter (learn is spam), SURBL filter (learn is spam), system white list (learn is not spam), and user white list (learn is not spam).

## Training using mbox files

Bayesian databases can be trained using mbox files, where one mbox file contains known spam email and one contains known clean email. Training using mbox files requires using email not previously processed by the Bayesian database that you want to train. Training with email that has passed through the Bayesian filter decreases the accuracy of the Bayesian filters.

## Training using control accounts

Bayesian databases can also be trained using the two control accounts, “learn is spam” and “learn is not spam”. The “learn is spam” control account trains databases with new spam messages. The “learn is not spam” control account trains databases to know those emails are not spam.

Training uses two control accounts; one is for spam and the other is for non-spam. Training the control accounts requires email not previously processed by the Bayesian filter because training with email that has passed through the Bayesian filter decreases the accuracy of the Bayesian filter.

The names of the control accounts can be customized by the administrator.

## Maintaining Bayesian databases

You need to maintain Bayesian databases to maximize the Bayesian filter’s effectiveness. Maintenance of the Bayesian database is done manually by correcting the Bayesian filter when it makes mistakes. Correcting a false positive or negative is done by sending the email to the control accounts on the FortiMail unit.

Names of the control accounts can be customized by the administrator.

## Black/white lists (system, session and personal)

The order of black/white lists has changed. White lists are now checked before black lists to allow white listing specific addresses within a black listed domain. For example, in FortiMail 2.8 and earlier releases, it was not possible to white list aabb@google.com and black list all other Google addresses since the black lists were checked first. A white list entry, such as aabb@google.com, would be ignored.

Black/white lists are now checked in the following sequence:

- 1 System sender white.
- 2 System sender black.
- 3 IP Session recipient white.
- 4 IP Session recipient black.
- 5 IP Session sender white.
- 6 IP Session recipient black.
- 7 User white.
- 8 User black.

## Greylist

You can now set the greylist initial expiry period from 4 to 24 hours, as well as modify the maximum number for greylist database entries.

The FortiMail-100 and FortiMail-400 unit entry range is 40 000 to 80 000, with the default range set at 40 000. FortiMail-2000 units and higher have a range of 80 000 to 125 000, with the default range set at 80 000. These entry range settings are only available in the CLI.

Default settings have also changed in FortiMail 3.0. The greylist period default value is now 10 minutes and the TTL default values are now 20 days.

The greylist feature is now bypassed in three specific circumstances:

- client appears in the access list with relay permission
- client establishes an authentication session
- client appears in greylist exempt list

Quarantine

## System Quarantine

The quarantine administrator now has web-based manager access to system quarantine. The quarantine administrator logs in the same way an administrator does when logging in to the FortiMail web-based manager. The quarantine administrator can view only system quarantine messages.

**Figure 12: Quarantine administrator viewing system quarantine spam messages**



Status	Subject	From	To	Rcpt To	Received	Size
<input type="checkbox"/>	test	"User One!" <user1@example.com>	<user1@example.com>	<user1@example.com>	Thu, 26 Jul 10:11 AM	1 k

FortiMail 3.0 also supports quarantine for outgoing email policies. You can enable quarantine for outgoing email policies by going to a policy (either recipient-based or IP based) and selecting the option, Quarantine to review, in the Action section.

## Log & Report

Log messages now include the word that triggered the banned word or dictionary check to the log data. The following is an example of a log message that recorded the banned word "garden".

```
2007-08-15 11:20:44 log_id=0501080300 type=spam
subtype=detected pri=information session_id=17FG8p5e000889
client_name=[172.16.120.2] from=spamsender@example.org
to=user1@example.com subject=Get free stuff! msg=Rejected by
BannedWord garden
```

The Logging menu also includes support for up to two Syslog servers or two FortiAnalyzer units. Multiple Syslog servers or FortiAnalyzer units are configured in **Log & Report > Log Setting**, Log to Remote Host section.

**Figure 13: Log settings for logging to two Syslog servers or FortiAnalyzer units**

## High Availability (HA)

A FortiMail network interface that is used for both user data and HA synchronization is not supported. It is recommended to keep HA isolated from your user network and to use the default HA interface for HA heartbeat and HA synchronization traffic. It is also recommended to use interfaces such as port 1 and port 2 for data traffic.

See the Fortinet Knowledge Center article, [Keep FortiMail HA heartbeat packets separate from data traffic](#), and [FortiMail Best Practices](#) for more information.

## Webmail

In Webmail, you can customize the Webmail login banner and HTTPS redirect of HTTP Webmail sessions is also available.

If you do not want to support HTTP WebMail access, you can configure HTTPS Webmail redirect. This option redirects users to connect to the HTTPS Webmail automatically, when they try to attempt to connect using HTTP Webmail.

You can now customize the webmail login banner string from the FortiMail web-based manager in **Mail Settings > Settings > Appearance**. For example, if you changed the default webmail login banner string to XYN\_Company, that name displays on the Webmail login page, as in Figure 9.

**Figure 14: A customized webmail login banner when logging in to the webmail interface**



# Managing firmware versions

Before upgrading to FortiMail 3.0, it is recommended to review this chapter so that you are fully aware of the procedures and issues when upgrading to this version. This chapter includes upgrading issues for all FortiMail 3.0 firmware versions and how to revert back to a previous firmware version, either to FortiMail 2.8 or earlier.

In addition to firmware images, Fortinet releases patch releases. A patch release is a firmware image that resolves specific issues without containing new features and/or changes to existing features. It is recommended to download and install a patch release as soon as it is released. When you install a patch release, you can use the same procedures as when upgrading to a current firmware image, including backing up your current configuration.

This chapter includes the following sections:

- [FortiMail 3.0 upgrade information](#)
- [Backing up your configuration](#)
- [Upgrading your FortiMail unit](#)
- [Reverting to a previous firmware version](#)



**Note:** FortiMail 3.0 supports upgrading from FortiMail 2.2 directly to FortiMail 3.0. The following upgrading procedures can be used with any firmware upgrade, regardless of the firmware version you want to upgrade to, for example, from FortiMail 2.2 to FortiMail 3.0.

## FortiMail 3.0 upgrade information

Before upgrading to FortiMail 3.0, it is important to read the following to learn about any limitations or additional support available for this operating system. This upgrade information carries forward to other firmware versions, such as FortiMail 3.0 MR1, unless otherwise stated.

### Loading default profiles

FortiMail 3.0 includes default antispam, antivirus and content profiles. After upgrading to FortiMail 3.0, you need to log in to the CLI and load the default profiles using the CLI command syntax, `execute factoryreset`. Before loading default profiles, it is recommended to back up your current FortiMail 3.0 configuration because the factory reset restores default settings and all current settings including emails are lost.



**Caution:** Always back up your configuration before upgrading, downgrading, or executing a factory reset. A factory reset restores all default settings, and all current settings, including emails, are lost. Backing up your configuration ensures that you can restore a current configuration.

## Configuration limits

The following configuration limits carry forward to FortiMail 3.0 MR1 and higher unless otherwise stated:

**Table 1: Configuration limits for all FortiMail units**

<b>FortiMail-100</b>	<ul style="list-style-type: none"> <li>• 50 email domains</li> <li>• 20 recipient-based policies per domain for incoming mail</li> <li>• 50 recipient-based policies for outgoing email</li> <li>• 20 IP-based policies</li> <li>• 60 AS profiles</li> <li>• 60 AV profiles</li> <li>• 60 Authentication profiles</li> <li>• 60 content profiles</li> <li>• 60 session profiles</li> <li>• 256 email aliases</li> <li>• 128 SMTP connections</li> <li>• 5 tiered administration domains</li> </ul>
<b>FortiMail-400</b>	<ul style="list-style-type: none"> <li>• 500 email domains</li> <li>• 40 recipient-based policies per domain for incoming mail</li> <li>• 500 recipient-based policies for outgoing email</li> <li>• 40 IP-based policies</li> <li>• 175 AS profiles</li> <li>• 175 AV profiles</li> <li>• 175 authentication profiles</li> <li>• 175 content profiles</li> <li>• 175 session profiles</li> <li>• 256 email aliases</li> <li>• 256 SMTP connections</li> <li>• 25 tiered administration domains</li> </ul>
<b>FortiMail-2000, 2000A and 4000A</b>	<ul style="list-style-type: none"> <li>• 3000 email domains (increased from 1500 in the previous versions)</li> <li>• 100 recipient-based policies per domain for incoming email</li> <li>• 1500 recipient-based policies for outgoing email</li> <li>• 100 IP-based policies</li> <li>• 550 AS profiles</li> <li>• 550 AV profiles</li> <li>• 550 authentication profiles</li> <li>• 550 content profiles</li> <li>• 550 session profiles</li> <li>• 256 email aliases</li> <li>• 512 SMTP connections</li> <li>• 50 tiered administration domains</li> </ul>

## Heuristic default setting changes (3.0 MR1)

Heuristic settings are now -20.000/3.500. It is recommended to review your heuristic settings, starting with the default thresholds.

## IP-based policy changes (3.0 MR2)

You will need to create appropriate recipient-based policies after upgrading if you enabled only IP-based policies for POP3 and Webmail in FortiMail 3.0 MR1 or lower. FortiMail 3.0 MR2 requires recipient-based policies because IP-based policies no longer check POP3 and Webmail access.

## Resetting to factory defaults in FortiMail 3.0 MR2

In FortiMail 3.0 MR2, there are two modes: basic management mode and advanced management mode. When the FortiMail unit is reset to factory default settings, the default mode is basic management mode. In this mode you can easily re-configure basic settings such as IP addresses, as well as switch back to advanced management mode.

## Backing up your configuration

Fortinet recommends backing up all configuration settings from your FortiMail unit(s) before upgrading to FortiMail 3.0. This ensures all configuration settings are not lost if you require downgrading to FortiMail 2.8 and want to restore those configuration settings.



**Caution:** Always back up your configuration before upgrading, downgrading, or executing a factory reset. A factory reset restores all default settings, and all current settings, including emails, are lost. Backing up your configuration ensures that you can restore a current configuration.

## Backing up your configuration using the web-based manager

The following procedure describes how to back up configuration settings and separately back up lists. Lists configured for Dictionary, Black/White List, as well as Bayesian databases, are not included in the backed up configuration file when you select Backup system settings on the System Setting Backup page.



**Note:** Session profile black/white lists are not included in the configuration backup file or the black/white list maintenance backup file. Session profile black/white lists are not affected when you backup, restore or reset.

### To back up configuration settings using the web-based manager

- 1 Go to **System > Status > Status**.
- 2 Under System Settings, select Backup.
- 3 Select Back up system settings.
- 4 Save the file to the management computer.
- 5 Select Return to go back to the Status page.

### To back up lists and Bayesian databases

- 1 Go to **Anti-Spam > Black/White List > Black/White List Maintenance**.  
This does not include session black/white lists.
- 2 Select Backup Black/White List.

- 3 Select Download Black/White List backup file, and save the file to the management computer.
- 4 Go to **Profile > Dictionary > Maintenance**.
- 5 Select Backup dictionary and save the file to the management computer.
- 6 Go to **Anti-Spam > Bayesian > DB Maintenance**.  
This backs up all Bayesian databases.
- 7 Select Backup bayesian database.
- 8 Select Download bayesian database backup file, and save the file to the management computer.

## Backing up your configuration using the CLI

You require a TFTP server when using the CLI to back up the current configuration. This procedure only backs up the configuration file. All lists are not backed up, and not all Bayesian databases, dictionary, and black/white lists.

It is recommended to back up the Bayesian database, dictionary and black/white lists separately as well. When backing up lists and the Bayesian database, use the procedure [“To back up lists and Bayesian databases” on page 37](#) since there are no CLI commands for backing up lists.

### To back up the configuration file using the CLI

Enter the following to back up the configuration:

```
execute backup config <filename> <tftp_ipv4>
```

This may take longer than a minute.

After successfully backing up your configuration file(s), either from the CLI or the web-based manager, proceed with upgrading to FortiMail 3.0.

## Upgrading your FortiMail unit

After backing up your current configuration, download the current firmware version from the support website before upgrading. All current, as well as previous, firmware versions are located at <http://support.fortinet.com>.

In the event upgrading to a current firmware version is unsuccessful, go to [“Reverting to a previous firmware version” on page 40](#) to downgrade to a previous firmware version.

### Upgrading to a current firmware version

The following procedures explain how to upgrade to any FortiMail 3.0 firmware version, using either the web-based manager or the CLI. After successfully upgrading to FortiMail 3.0 or higher, the current antivirus definitions are replaced with definitions included in the new firmware release; you need to update the antivirus definitions to ensure they are current. See the *FortiMail Administration Guide* to update antivirus definitions.

After upgrading to FortiMail 3.0, you will need to create new LDAP profiles because LDAP profiles do not carry forward to FortiMail 3.0. See the *FortiMail Administration Guide* to create LDAP profiles.

You require a TFTP server when using the CLI to upgrade to a current firmware version.

You can use the following procedures when installing a patch release. A patch release is a firmware image that resolves specific issues without containing new features and/or changes to existing features. You can install a patch release whether you upgraded to the current firmware version or not.



**Caution:** Always back up your configuration before upgrading, downgrading, or executing a factory reset. A factory reset restores all default settings, and all current settings, including emails, are lost. Backing up your configuration ensures that you can restore a current configuration.

#### To upgrade to a current firmware version using the web-based manager

- 1 Copy the firmware, previously downloaded from the support website, to the root directory of the TFTP server.
- 2 Log in to the web-based manager.
- 3 Go to **System > Status > Status**.
- 4 Under Unit Information, beside Firmware Version, select Update.
- 5 Enter the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.

The FortiMail unit uploads the firmware image file, upgrades to the new firmware version, reboots, and displays the login. This process takes longer than one minute.

See [“Verifying the upgrade” on page 40](#) to re-connect to the FortiMail unit and verify that the upgrade was successful.

#### To upgrade to a current firmware version using the CLI

- 1 Copy the firmware, previously downloaded from the support website, to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log in to the CLI.
- 4 Enter the following to ping the computer running the TFTP server:

```
execute ping <tftp_ipv4>
```

Pinging the computer running the TFTP server verifies that the FortiMail unit and TFTP server are successfully connected.

- 5 Enter the following to copy the firmware image from the TFTP server to the FortiMail unit:

```
execute restore image <name_str> <tftp_ipv4>
```

Where <name\_str> is the name of the firmware image file and <tftp\_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.1.68`, enter:

```
execute restore image.out 192.168.1.68
```

- 6 The FortiMail unit responds with a message similar to the following:

```
This operation will replace the current firmware version!
Do you want to continue?(y/n)
```

- 7 Enter `y`.

The FortiMail unit uploads the firmware image file, upgrades to the new firmware version, and reboots. This process takes a few minutes.

- 8 Log back in to the CLI.

- 9 Enter the following to confirm the firmware image successfully installed:

```
get system status
```

See [“Verifying the upgrade” on page 40](#) to verify that configuration settings carried forward.

## Verifying the upgrade

You will want to verify that configuration settings carried forward after successfully upgrading to the current firmware version. Verifying configuration settings provides familiarity with the new features and changes in the current firmware release.

### To verify the upgrade

- 1 Clear your browser’s cache and refresh the page.
- 2 Log in to the web-based manager using `/admin` at the end of the URL address. For example:  
`http://172.31.100.165/admin`
- 3 Go through each menu to verify that the configuration settings carried forward.
- 4 Configure settings that did not carry forward, for example, LDAP profiles.

## Reverting to a previous firmware version

You may need to revert to a previous firmware version if the upgrade did not install successfully. The following sections will help you to downgrade to FortiMail 2.8 MR1 and restore your previous configuration.



**Caution:** Always back up your configuration before upgrading, downgrading, or executing a factory reset. A factory reset restores all default settings, and all current settings, including emails, are lost. Backing up your configuration ensures that you can restore a current configuration.

## Downgrading to a previous firmware version

When downgrading the firmware, all configuration settings are lost. It is recommended to back up your current configuration in the event you want to try upgrading to the new firmware version again. You may want the current FortiMail 3.0 configuration in the event you decide to upgrade to FortiMail 3.0 again.

The following procedures enable you to downgrade to FortiMail 2.8 MR1 using either the web-based manager or CLI.

### To downgrade using the web-based manager

- 1 Copy the firmware, previously downloaded and saved from the support website, to the root directory of the TFTP server.
- 2 Log in to the web-based manager.
- 3 Go to **System > Status > Status**.
- 4 Under Unit Information, beside Firmware Version, select Update.
- 5 Enter the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.

The FortiMail unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the login. This process takes a few minutes.

After downgrading successfully to FortiMail 2.8MR1, you will need to re-enter the internal IP address because it reverts to the default setting, 192.168.1.99. See ["Reconnecting to the FortiMail unit" on page 42](#) for more information.

### To downgrade using the CLI

- 1 Copy the firmware, previously downloaded and saved from the support website, to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log in to the CLI.
- 4 Enter the following to ping the computer running the TFTP server:

```
execute ping <tftp_ipv4>
```

Pinging the computer running the TFTP server verifies that the FortiMail unit and TFTP server are successfully connected.

- 5 Enter the following to copy the firmware image from the TFTP server to the FortiMail unit:

```
execute restore image <name_str> <tftp_ipv4>
```

When <name\_str> is the name of the firmware image file and <tftp\_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.68, enter:

```
execute restore image.out 192.168.1.68
```

- 6 The FortiMail unit responds with a message similar to the following:

```
This operation will downgrade the current firmware version!  
Do you want to continue?(y/n)
```

- 7 Enter `y`.  
The FortiMail unit uploads the firmware image file, downgrades to the new firmware version, and reboots. This process may take a few minutes.
- 8 Log back in to the CLI.
- 9 Enter the following to confirm the firmware image successfully installed:  

```
get system status
```

Reconnect to the FortiMail unit by following the next procedure.

## Reconnecting to the FortiMail unit

After successfully downgrading to a previous firmware version, the FortiMail unit reverts to factory default settings. This includes the internal IP address that connects you to the FortiMail web-based manager.

Use the following procedures whenever the FortiMail unit has been reset to factory defaults and you need to reconnect to the FortiMail unit.

### To reconnect to the FortiMail unit using the LCD interface

- 1 Press Enter to display the Main Menu.
- 2 Press Enter to display the interface list.
- 3 Use the up or down arrows to highlight the internal interface and press Enter.
- 4 Press Enter for IP Address.
- 5 Use the up and down arrows to increase or decrease each number of each IP address digit. Press Enter to go to the next IP address digit or press Esc to move to the previous digit.
- 6 After selecting the last IP address digit, press Enter to save the IP address.
- 7 Repeat steps 4 to 7 to enter the netmask address for the internal interface.
- 8 After selecting the last netmask address digit, press Enter to save the netmask address.
- 9 Press Esc to return to the Main Menu.

### To reconnect to the FortiMail unit using the CLI

- 1 Log in to the CLI.
- 2 Enter the following to set the internal IP address:  

```
set system interface <interface_name> mode static ip  
<interface_ipv4> <ipv4_mask>
```
- 3 Enter the following to set the allow access settings for the internal IP address:  

```
set system interface <interface_name> config allowaccess  
ping http https
```
- 4 Log in to the web-based manager.
- 5 Go to **System > Status > Status** to verify that the firmware downgraded.

## Restoring the previous configuration

You can restore your configuration settings that were saved previously, before upgrading to a new firmware version.

You require a TFTP server if restoring the configuration using the CLI.

### To restore configuration settings using the web-based manager

- 1 Clear your browser's cache and refresh the browser.
- 2 Log in to the web-based manager.
- 3 Go to **System > Status > Status**.
- 4 Under System Settings, select Restore.
- 5 Enter the file name or select Browse to locate the file.
- 6 Select OK.

The FortiMail unit restores the previous configuration settings, and reboots. This may take longer than a minute.

### To restore configuration settings using the CLI

- 1 Log in to the CLI.
- 2 Enter the following to restore the previous configuration settings:

```
execute restore config <file_name> <tftp_ipv4>
```

The following message appears:

```
This operation will overwrite the current settings!  
(The current admin password will be preserved.)  
Do you want to continue? (y/n)
```

- 3 Enter `y`.

The FortiMail unit restores the previous configuration settings, and reboots. This may take a few minutes.

You can verify that the configuration settings are restored by logging in to the web-based manager and going through the various menus and tabs.



# Index

## A

administration changes, 3.0MR2 12  
 advanced mode, 3.0MR2 15  
 auto-training bayesian databases, 3.0 30

## B

backing up  
   using the CLI 38  
   using web-based manager 37  
 backing up configuration 37  
 basic management mode, 3.0MR2 13  
 basic mode, 3.0MR2 13  
 bayesian filtering, 3.0 30  
 black/white lists, 3.0 31

## C

CLI  
   backing up 38  
 config wizard, 3.0MR2 13  
 configuration limits, 3.0 36  
 control accounts for bayesian training, 3.0 31  
 custom messages for spam, av and content filtering, 3.0 28  
 customer service 9

## D

ddns support, 3.0 27  
 documentation  
   FortiMail 8  
 domain configuration, 3.0 27  
 Downgrading 41  
 downgrading  
   using web-based manager 41  
 downgrading to previous firmware 41

## E

email alias support, 3.0 28  
 email header information, 3.0 27

## F

Fortinet customer service 9

## G

greylist checking, 3.0 32

## H

ha, 3.0 33  
 ha, 3.0MR2 18  
 history logs, 3.0MR2 18

## I

image scanning, 3.0 29  
 ip policy changes, 3.0MR2 16

## L

loading default profiles, 3.0 35  
 log & report (basic), 3.0MR2 15  
 log & report menu in basic mode, 3.0MR2 15  
 log&report, 3.0 32

## M

mail queue default settings, 3.0MR2 15  
 maintaining bayesian databases, 3.0 31  
 management (basic), 3.0MR2 14  
 management menu in basic mode, 3.0MR2 14  
 mbox files, bayesian training 3.0 31  
 multiple language support for profiles, 3.0 29

## N

new features and changes, 3.0 25  
   auto-training bayesian databases 30  
   bayesian filtering 30  
   black/white lists (system, session and personal) 31  
   ddns support 27  
   domain configuration 27  
   email alias support 28  
   email header information 27  
   greylist checking 32  
   ha 33  
   image scanning 29  
   log&report 32  
   maintaining bayesian databases 31  
   mbox files, bayesian training 31  
   multiple language support, profiles 29  
   policies 29  
   quarantine 32  
   regex support, profiles 29  
   relay server support 27  
   spam and summary email report custom formats 28  
   spam, av and content filtering custom messages 28  
   using control accounts, bayesian training 31  
   webmail 33  
 new features and changes, 3.0MR1 11, 21  
   deep header analysis 22  
   deep header scanning 22  
   dynamic heuristic rules 23

- dynamic heuristic rules 23
- PDF scanning 22
- new features and changes, 3.0MR2
  - administration changes 12
  - advanced management mode 15
  - advanced mode 15
  - basic management mode 13
  - basic mode 13
  - config wizard 13
  - ha 18
  - history logs 18
  - ip policy changes 16
  - log & report (basic) 15
  - log & report, basic mode 15
  - mail queue default settings 15
  - management, basic mode 14
  - managment (basic) 14
  - predefined reports 17
  - predefined reports (basic) 17
  - quick start wizard 13
  - re-order of log type tabs 18
  - re-ordering of log type tabs 18
  - settings (basic) 15
  - settings, basic mode 15

## P

- policies, 3.0 29
- predefined reports (basic), 3.0MR2 17
- predefined reports, 3.0MR2 17

## Q

- quarantine, 3.0 32
- quick start wizard, 3.0MR2 13

## R

- reconnecting to the FortiMail unit 42
- regex support for profiles, 3.0 29
- relay server support, 3.0 27
- re-order of log type tabs, 3.0MR2 18
- re-ordering of log type tabs, 3.0MR2 18
- restoring previous configuration 43

## S

- settings (basic), 3.0MR2 15
- settings menu in basic mode, 3.0MR2 15
- spam and summary email report custom formats, 3.0 28
- support
  - customer service and technical 9

## T

- technical support 9

## U

- upgrade information, 3.0 35
  - configuration limits 36
  - loading default profiles 35
- upgrading
  - FortiMail unit 38
- upgrading to current firmware version 38

## V

- verifying the upgrade 40

## W

- web-based manager
  - backing up 37
  - downgrading 41
- webmail, 3.0 33

**FORTINET**<sup>™</sup>

[www.fortinet.com](http://www.fortinet.com)

**FORTINET™**

[www.fortinet.com](http://www.fortinet.com)