

*FortiGate<sup>®</sup> Multi-Threat Security System*

*Release Notes*  
*v4.0 MR3*

01-430-84420-20110318

**FORTINET<sup>®</sup>**

## Table of Contents

1	FortiOS v4.0 MR3	1
1.1	Summary of Enhancements Provided by v4.0 MR3	1
2	Special Notices	5
2.1	General	5
2.2	Possibly lost access after downgrade	5
2.3	Logging to FortiAnalyzer	5
2.4	Rename FSAE to FSSO	6
3	Upgrade Information	7
3.1	Upgrading from FortiOS v3.00 MR7	7
3.2	Upgrading from FortiOS v4.0	7
3.3	Upgrading from FortiOS v4.0 MR1	7
4	Downgrading to FortiOS v4.0.0	9
5	Fortinet Product Integration and Support	10
5.1	FortiManager Support	10
5.2	FortiAnalyzer Support	10
5.3	FortiClient Support	10
5.4	Fortinet Single Sign On(FSSO) Support	10
5.5	AV Engine and IPS Engine Support	10
5.6	3G MODEM Support	10
5.7	AMC Module Support	12
5.8	SSL-VPN Support	13
5.8.1	SSL-VPN Standalone Client	13
5.8.2	SSL-VPN Web Mode	13
5.9	SSL-VPN Host Compatibility List	14
5.10	Explicit Web Proxy Browser Support	15
5.11	FortiExplorer Support	15
6	Resolved Issues in FortiOS v4.0 MR3	16
6.1	Command Line Interface (CLI)	16
6.2	Web User Interface	16
6.3	System	17
6.4	High Availability	18
6.5	Router	19
6.6	Firewall	19
6.7	IPS	19
6.8	VPN	19
6.9	Web Filter	21
6.10	Instant Message	21
6.11	WAN Optimization	21
6.12	Log & Report	22
6.13	Wi-Fi	22
7	Known Issues in FortiOS v4.0 MR3	23
7.1	Web User Interface	23
7.2	System	23
7.3	High Availability	23
7.4	Firewall	23
7.5	Web Filter	23

<a href="#">7.6 Antispam.....</a>	<a href="#">24</a>
<a href="#">7.7 VPN.....</a>	<a href="#">24</a>
<a href="#">7.8 Log &amp; Report.....</a>	<a href="#">24</a>
<a href="#">7.9 FSAE Windows DC Agent.....</a>	<a href="#">24</a>
<a href="#">7.10 Web Proxy.....</a>	<a href="#">24</a>
<a href="#">8 Image Checksums.....</a>	<a href="#">25</a>

*Change Log*

Date	Change Description
2011-03-18	Initial Release.

© Copyright 2011 Fortinet Inc. All rights reserved.  
Release Notes FortiOS™ v4.0 MR3.

**Trademarks**

Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, 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 FortiOS v4.0 MR3

This document provides installation instructions, and addresses issues and caveats in FortiOS™ v4.0 MR3 B0441 release. The following outlines the release status for several models.

Model	FortiOS v4.0 MR3 Release Status
FGT-30B, FWF-30B, FGT-50B, FGT-51B, FWF-50B, FGT-60B, FWF-60B, FGT-60C, FGT-80C, FGT-80CM, FWF-80CM, FWF-81CM, FGT-82C, FGT-100A, FGT-110C, FGT-111C, FGT-200A, FGT-200B, FGT-200B-POE, FGT-224B, FGT-300A, FGT-310B, FGT-311B, FGT-310B-DC, FGT-400A, FGT-500A, FGT-620B, FGT-620B-DC, FGT-621B, FGT-800, FGT-800F, FGT-1000A, FGT-1000A-FA2, FGT-1000A-LENC, FGT-1240B, FGT-3000, FGT-3016B, FGT-3040B, FGT-3140B, FGT-3600, FGT-3600A, FGT-3810A, FGT-3950B, FGT-3951B, FGT-5001A, FGT-5001, FGT-5001FA2, FGT-5002FB2, FGT-5005FA2, FGT-ONE and FGT-VM.	All models are supported on the regular v4.0 MR3 branch.

Please visit <http://docs.forticare.com/fgt.html> for additional documents on FortiOS v4.0 MR3 release.

## 1.1 Summary of Enhancements Provided by v4.0 MR3

The following is a brief list of the new features added in FortiOS v4.0 MR3.

- The following is a brief list of the new features added in FortiOS v4.0 MR3.
- Supports "Local In" Policies to and from the FortiGate
- Introduces Unified AV Engine
- Supports Configuration Object Tagging
- Introduces Configuration Rollback feature
- Supports Explicit FTP proxy
- Enhanced Explicit Proxy feature to support Proxy Chaining
- Supports FAS (previously known as FAMS) and FortiAnalyzer Logging Extensions
- Flow-based DLP Support
- Flow-based Web Content Filtering
- Supports IPv6 Firewall offload feature on ASM-CE4, ADM-XE2 and ADM-FB8 modules
- FTPS protocol support for SSL Inspection feature
- Supports Log Viewer Filters
- Network Scan feature Improvements
- Supports Per-VDom Configuration Files
- Policy Table web UI Improvements
- Introduces 'Port Pair' feature in Transparent mode
- Supports SSL-VPN Client in Port Forward mode
- Enhanced User Authentication feature
- Extends Wireless Controller feature support to FortiAP-220A and FortiAP-220B
- Introduces 2-Factor Authentication
- Supports Dynamic Profiles
- Added support for Pictures in Replacement Messages

- Authentication Page Style Improvements
- Enhanced Logging feature
- Supports Configuration Restore via SCP Protocol
- Improved Dashboard Widgets
- Supports DHCP Address Reservation
- Support for DHCP6
- Endpoint NAC Improvement
- Facebook Application Control
- Firewall Schedule Enforcement
- FortiASIC traffic offload Improvements
- HTTP Host Load Balancing
- Improved Chart Display
- Improved Firewall Session Control
- Firewall Session Control Improvements
- IPS Sensor Enhancements
- Supports IPS Signature Search and IPS Signature Threshold
- IPSec 'get' Command Improvement
- IPv6 Firewall Authentication
- Added IPv6 SNMP Support
- Traffic Logging Improvements
- Modem Interface Improvements
- MultiCast IGMP Static Join and PIM Enhancement
- Session Table Enhancements
- NTLM Authentication Extensions
- Supports Per-IP Traffic Shaping for Application Control
- Firewall Policy Enhancements
- Proxy Support with SSL Offload
- RADIUS Accounting Extension
- 'Top Session widget' supports IPv6 sessions
- Simplify Report Configuration
- SNMP Enhancements including web UI support for SNMPv3
- Various web UI consolidation and Enhancements
- SSL-VPN Tunnel Widget Improvements
- Supports SSL-VPN Web Mode over IPv6
- Supports SSL-VPN Policy DE-Authentication
- Static Route web UI Improvements
- Supports sub-second Failover for NP4 Ports
- Supports Authentication Group Matching for TACACS+
- Troubleshooting Improvement
- SQL Logging Enhancements
- VRRP Virtual MAC Support
- Enhanced Web Filter Override feature
- Weighted HA Failover Improvements
- WiFi Enterprise Authentication Support
- Supports per-zone option for Local DNS Server
- Explicit Proxy Improvements
- Supports Hosted NAT traversal for RTP pin-holing
- Introduced Quotas for Web Cache / Byte Cache
- Supports Password Renewal for LDAP Users over SSLVPN
- Supports FMC-XG2 Module
- Generate protocol identification tag for FDN reporting on AV
- Extension of SP acceleration to support offloading of interface-based IPS
- Support for Monitoring Dynamic Data on FMG

- Support for Internet Content Adaptation Protocol (ICAP)
- PKI Authentication Extensions (Merge Top3 1359)
- Merge UTM Logs into one Category
- Configurable Global Admin Profiles
- Add monitor section in menu system
- Support IPS one-arm on XLR
- Inter-Product Secure Communications
- DiffServ per Application Filter
- DLP: Document Fingerprinting
- Geography-based Filtering
- FortiGate Default Report
- Endpoint NAC Extension
- Rogue AP Detection & Reporting
- Captive Portal for Wifi Authentication
- Rogue AP Suppression
- Distributed ARRP (automatic radio resource provisioning)
- Simplify Email Filtering
- ELBCv3 graceful firmware upgrade
- File Filter Reorganization
- SHA-384 and SHA-512 support to IKE and IPsec
- SSL Proxy: Verify Host SSL Certificates
- Dynamic Profile & Endpoint Filter Extensions
- Replacement Message Reorganization
- DNS zone transfer and dns forwarder feature
- Setup Wizard for FOS
- Simple Forticlient VPN GUI
- Web Filter Improvement
- Web Filtering Disclaimer
- Web Filter Category Reorg
- Report Editor Improvements
- FortiGate Default Report - Improvements

## 2 Special Notices

### 2.1 General

The TFTP boot process erases all current firewall configuration and replaces it with the factory default settings.

---

#### **IMPORTANT!**

##### **Monitor Settings for Web User Interface Access**

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

##### **Web Browser Support**

- Microsoft Internet Explorer™ 8.0 (IE8) and FireFox 3.5 or later are fully supported.

##### **BEFORE any upgrade**

- **[FortiGate Configuration]** Save a copy of your FortiGate unit configuration (including replacement messages) prior to upgrading.

##### **AFTER any upgrade**

- **[WebUI Display]** If you are using the Web UI, clear the browser cache prior to login on the FortiGate to ensure proper display of the Web UI screens.
- **[Update the AV/IPS definitions]** The AV/IPS signature included with an image upgrade may be older than ones currently available from the Fortinet's FortiGuard system. Fortinet recommends performing an "Update Now" as soon as possible after upgrading. Consult the FortiGate User Guide for detailed procedures.

---

### 2.2 Possibly lost access after downgrade

There is new accessible option called `FMG-Access` under system interface introduced on 4.3. If the option is enabled on the interface that administrator uses to access FortiGate, firewall administrators could lose their access to web UI after FortiGate is downgraded to 4.2 or below. The reason is that former FOS versions do not have this option and hence system will reset the access options to be factory default of the interface that has `FMG-Access` on under 4.3. Thus some interfaces may only have `ping` option enabled and the rest of the options will be unavailable.

Workaround is to disable `FMG-Access` option for particular interface before the downgrade happens.

### 2.3 Logging to FortiAnalyzer

From this release FortiGate users can enjoy a encrypted communication between FortiGate and FortiAnalyzer in high, low, default and none encrypted options. Both sides need to have 4.3 or above running on the boxes to support this feature. If FortiAnalyzer is running on 4.2 it does not support encrypted communication yet. When FortiGate is upgrade from 4.2 to 4.3, there is no problem for the communication because encryption option is disabled by default after upgrade. However, if a FortiGate have a fresh burned 4.3 image directly, the encryption option will be turned on by default. Thus some users may want to use the following CLI commands to change the option if they have communication issue between FortiGate and FortiAnalyzer,

```
config log fortianalyzer setting
```

```
    set enc-algorithm disable
end
```

## 2.4 Rename FSAE to FSSO

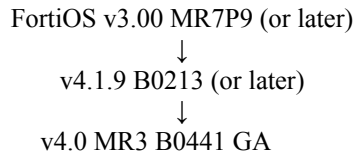
FSAE will now be renamed as FSSO—Fortinet Single Sign On and all FSAE name related configurations will be changed to FSSO. Users will find name changes under Firewall---Identity Firewall policy, User---User Group, etc. Detailed information will be released in technical document.



## 3 Upgrade Information

### 3.1 Upgrading from FortiOS v3.00 MR7

Direct upgrading from FortiOS v3.00 MR7 Patch Release 9 to v4.0 MR3 is not supported. Fortinet recommends the following upgrade path:



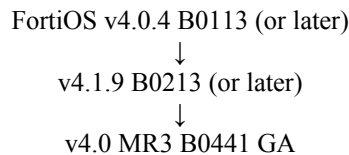
After every upgrade, ensure that the build number and branch point match the image that was loaded.

### 3.2 Upgrading from FortiOS v4.0

FortiOS v4.0 MR3 officially supports upgrade from the FortiOS v4.0 Patch Release 4 or later. See the upgrade path below. The arrows indicate "upgrade to".

#### [FortiOS v4.0]

The upgrade is supported from FortiOS v4.0.4 B0113 or later.



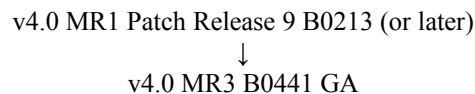
After every upgrade, ensure that the build number and branch point match the image that was loaded.

### 3.3 Upgrading from FortiOS v4.0 MR1

FortiOS v4.0 MR3 officially supports upgrade from the FortiOS v4.0 MR1 Patch Release 4 or later. See the upgrade path below. The arrows indicate "upgrade to".

#### [FortiOS v4.0 MR1]

The upgrade is supported from FortiOS v4.0 MR1 Patch Release 4 B0196 Patch Release 4 or later.



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

#### [DLP Rule]

A DLP rule with subprotocol setting set to 'sip simple sccp' will be lost upon upgrading to FortiOS v4.0 MR3.

#### [HTTPS Invalid Certificate Setting]

The HTTPS "allow-invalid-server-cert" setting under "config firewall profile" will be lost after upgrading from FortiOS v4.0 MR1 Patch Release 3 B0194 to FortiOS v4.0 MR3 B0441.

#### [AlertMail Setting]

The "set local-disk-usage-warning enable" setting under "config alertemail settings" will get reset to disable after upgrading to FortiOS v4.0 MR3.

**[System Autoupdate Settings]**

The settings under "config system autoupdate schedule" will get set to default values after upgrading to FortiOS v4.0 MR3.

## 4 Downgrading to FortiOS v4.0.0

Downgrading to FortiOS v4.0.0 GA (or later) results in configuration loss on ALL models. Only the following settings are retained:

- operation modes
- interface IP/management IP
- route static table
- DNS settings
- VDom parameters/settings
- admin user account
- session helpers
- system access profiles

## 5 Fortinet Product Integration and Support

### 5.1 FortiManager Support

FortiOS v4.0 MR3 is supported by FortiManager v4.0 MR2 Patch 6.

### 5.2 FortiAnalyzer Support

FortiOS v4.0 MR3 is supported by FortiAnalyzer v4.0 MR2 Patch 3.

### 5.3 FortiClient Support

FortiOS v4.0 MR3 is fully compatible with FortiClient v4.0 MR2 Patch 3.  
FortiOS v4.0 MR3 is backward compatible with FortiClient v4.1.3 or later.

**Note:** Although FortiOS v4.0 MR3 is compatible with FortiClient v4.1.3 there is a possibility that some features may not be supported.

FortiOS v4.0 MR3 is supported by FortiClient v4.0 MR3 for the following:

- 32-bit version of Microsoft Windows XP
- 32-bit version of Microsoft Windows Vista
- 64-bit version of Microsoft Windows Vista
- 32-bit version of Microsoft Windows 7
- 64-bit version of Microsoft Windows 7

### 5.4 Fortinet Single Sign On(FSSO) Support

FortiOS v4.0 MR3 is supported by FSSO v3.00 B066 (FSAE collector agent 3.5.066) for the following:

- 32-bit version of Microsoft Windows 2003 R1 Server
- 64-bit version of Microsoft Windows 2003 R1 Server
- 32-bit version of Microsoft Windows 2008 R1 Server
- 64-bit version of Microsoft Windows 2008 R1 Server
- 64-bit version of Microsoft Windows 2008 R2 Server
- Novell E-directory 8.8.

IPv6 currently is not supported by FSSO.

### 5.5 AV Engine and IPS Engine Support

FortiOS v4.0 MR3 is supported by AV Engine 4.00257 and IPS Engine 1.00224.

### 5.6 3G MODEM Support

The following models and service providers were tested.

Service Provider	3G Card	Identification (IMEI)	Datacard Firmware
<b>Canada</b>			
Telus	ZTE MY39	-	P650M1V1.0.2_Telus_060331
Rogers	Option Globetrotter Qualcomm 3G GX0202	352115011023553	1.10.8Hd

Service Provider	3G Card	Identification (IMEI)	Datacard Firmware
Rogers	Huawei E220	358191017138137	11.110.05.00.00
Rogers	Sierra AirCard 595	-	p1906000,5077
<b>EMEA</b>			
Swisscom	Huawei E1692	353435024553159	11.104.16.81.00
Sunrise	Huawei E180 *	356185039363519	11.104.16.00.154
Swisscom	Sierra Aircard 880	354217010372813	-
<b>APAC</b>			
E-Mobile	NEC Infrontia Corporation D01NE	-	-
E-Mobile	NEC Infrontia Corporation D02NE	-	-
E-Mobile	Longcheer Holdings Limited D11LC	353780020859740	LQA0012.1.2_M533A
E-Mobile	Huawei D23HW	351700030381719	11.112.15.03.00
<b>AMER</b>			
Telecom	Sierra Compass 597	-	Rev 1.0 (2), p2314500,4012
Optus	Huawei E169	358109021556466	11.314.17.00.00
Hutchison/3	Huawei E220	358191017339891	11.117.09.00.100
Telecom	Sierra 597E	-	p2102900,4012
Vodafone	Huawei E220	354136020989038	11.117.09.04.00
Soul/TPG	Huawei E220	358193016941644	11.117.08.00.00
Telstra	Option GE0202	356812010493268	2.5.2Hd
Telstra	Sierra 880E	356812010493268	F1_0_0_9AP C:/WS/FW/F1_0_0_9AP/MSM72 00R3/SRC/AMSS
Telstra	Sierra AC501/Sierra 880E+	358248020068162	K2_0_7_1BAP C:/WS/FW/K2_0_7_1BAP/MSM 6290/SRC
Telstra	Sierra AC875	352822010757236	H2_0_6_0ACAP C:/WS/FW/H2_0_6_0ACAP/MS M6280/SRC
Telstra	Sierra USB 306	359475020397478	M2_0_4_0AP C:/WS/FW/M2_0_4_0AP/MDM8 200/SRC/AMSS
Telecom New Zealand	Sierra Compass 885	35992013540914	1_0_1_17AP C:/WS/FW/J1_0_1_17AP/MSM7 200A/SRC/AMSS
AT&T	Sierra Wireless AC881	354218012004149	F1_0_0_4AP C:/WS/FW/F1_0_0_4AP/MSM72 00R3/SRC/AMSS
Bell Mobility	Novatel / Ovation U727	ESN: 0x5B80428F	m6800B-RAPTOR65_B-126
Sprint	Sierra Wireless 250U	09611172048	p3012801,60767

\* The FortiGate may display the modem name as Huawei E220

## 5.7 AMC Module Support

FortiOS v4.0 MR3 supports AMC removable modules. These modules are not hot swappable. The FortiGate must be turned off before the module is inserted or removed.

AMC Modules	FortiGate Support
Internal Hard Drive (ASM-S08)	FGT-310B FGT-620B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW
Single Width 4-port 1Gbps Ethernet interface (ASM-FB4)	FGT-310B FGT-311B FGT-620B FGT-1240B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW
Dual Width 2-port 10Gbps Ethernet interface (ADM-XB2)	FGT-3810A FGT-5001A-DW
Dual Width 8-port 1Gbps Ethernet interface (ADM-FB8)	FGT-3810A FGT-5001A-DW
Single Width 2-port Fiber 1Gbps bypass interface (ASM-FX2)	FGT-310B FGT-311B FGT-620B FGT-1240B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW
Single Width 4-port Ethernet bypass interface (ASM-CX4)	FGT-310B FGT-311B FGT-620B FGT-1240B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW
AMC Security Processing Engine Module (ASM-CE4)	FGT-1240B FGT-3810A FGT-3016B FGT-5001A-SW
AMC Security Processing Engine Module (ADM-XE2)	FGT-3810A FGT-5001A-DW
Rear Transition Module (RTM-XD2)	FGT-5001A-DW to support RTM-XD2
Four Port T1/E1 WAN Security Processing Module (ASM-	FGT-310B

AMC Modules	FortiGate Support
ET4)	FGT-311B
Rear Transition Module (RTM-XB2)	FGT-5001A-DW to support RTM-XB2
Security Processing Module (FMC-XG2)	FGT-3950B FGT-3951B FGT-3040B FGT-3140B
Security Processing Module (FMC-C20)	FGT-3950B FGT-3951B
Security Processing Module (FMC-F20)	FGT-3950B FGT-3951B

## 5.8 SSL-VPN Support

### 5.8.1 SSL-VPN Standalone Client

FortiOS v4.0 MR3 supports the SSL-VPN tunnel client standalone installer B2138 for the following:

- Windows in .exe and .msi format
- Linux in .tar.gz format
- Mac OS X in .dmg format
- Virtual Desktop in .jar format for Windows 7, XP, and Vista

The following Operating Systems are supported.

Windows	Linux	Mac OS X
Windows XP 32-bit SP2	CentOS 5.2 (2.6.18-el5)	Leopard 10.6.3
Windows XP 64-bit SP1	Ubuntu 8.0.4 (2.6.24-23)	
Windows Vista 32-bit SP1		
Windows Vista 64-bit SP1		
Windows 7 32-bit		
Windows 7 64-bit		
Virtual Desktop Support		
Windows XP 32-bit SP2		
Windows Vista 32-bit SP1		
Windows 7 32-bit		

### 5.8.2 SSL-VPN Web Mode

The following browsers and operating systems are supported by SSL-VPN web mode.

Operating System	Browser
Windows XP 32-bit SP2	IE7, IE8, and FF 3.6
Windows XP 64-bit SP1	IE7 and FF 3.6
Windows Vista 32-bit SP1	IE7, IE8, and FF 3.6
Windows Vista 64-bit SP1	IE7 and FF 3.6
Windows 7 32-bit	IE8 and FF 3.6
Windows 7 64-bit	IE8 and FF 3.6
CentOS 5.2 (2.6.18-el5)	FF 1.5 and FF 3.0
Ubuntu 8.0.4 (2.6.24-23)	FF 3.0
Mac OS X Leopard 10.5	Safari 4.1

## 5.9 SSL-VPN Host Compatibility List

The following Antivirus and Firewall client software packages are supported.

Product	Antivirus	Firewall
<b>Windows XP</b>		
Symantec Endpoint Protection v11	✓	✓
Kaspersky Antivirus 2009	✓	✗
McAfee Security Center v8.1	✓	✓
Trend Micro Internet Security Pro	✓	✓
F-Secure Internet Security 2009	✓	✓

Product	Antivirus	Firewall
<b>Windows 7 (32bit)</b>		
CA Internet Security Suite Plus Software	✓	✓
AVG Internet Security 2011	✗	✗
F-Secure Internet Security 2011	✓	✓
Kaspersky Internet Security 2011	✓	✓
McAfee Internet Security 2011	✓	✓
Norton 360™ Version 4.0	✓	✓
Norton™ Internet Security 2011	✓	✓
Panda Internet Security 2011	✓	✓
Sophos Security Suite	✓	✓
Trend Micro Titanium Internet Security	✓	✓



Product	Antivirus	Firewall
ZoneAlarm Security Suite	√	√
Symantec Endpoint Protection Small Business Edition 12.0	√	√

Product	Antivirus	Firewall
<b>Windows 7 (64bit)</b>		
CA Internet Security Suite Plus Software	√	√
AVG Internet Security 2011	✗	✗
F-Secure Internet Security 2011	√	√
Kaspersky Internet Security 2011	√	√
McAfee Internet Security 2011	√	√
Norton 360™ Version 4.0	√	√
Norton™ Internet Security 2011	√	√
Panda Internet Security 2011	√	√
Sophos Security Suite	√	√
Trend Micro Titanium Internet Security	√	√
ZoneAlarm Security Suite	√	√
Symantec Endpoint Protection Small Business Edition 12.0	√	√

## 5.10 Explicit Web Proxy Browser Support

The following browsers are supported by Explicit Web Proxy feature.

Supported Browser
Internet Explorer 7
Internet Explorer 8
FireFox 3.x

## 5.11 FortiExplorer Support

FortiOS v4.0 MR3 is supported by FortiExplorer 1.3.1205.

## 6 Resolved Issues in FortiOS v4.0 MR3

The resolved issues listed below does not list every bug that has been corrected with this release. For inquires about a particular bug, contact Customer Support.

### 6.1 Command Line Interface (CLI)

**Description:** End user is able to assign an IP with 32 bit net mask to management IP in TP mode via CLI.

**Bug ID:** 123965

**Status:** Fixed in v4.0 MR3.

**Description:** Static ARP entry will be configurable under CLI for TP mode.

**Bug ID:** 133930

**Status:** Fixed in v4.0 MR3.

**Description:** New CLI command to customize the number of failed authentication attempts is added.

**Bug ID:** 117822

**Status:** Fixed in v4.0 MR3.

**Description:** New options `fp-anomaly` and `fp-disable` shall be removed on non-AMC interfaces.

**Bug ID:** 128744

**Status:** Fixed in v4.0 MR3.

### 6.2 Web User Interface

**Description:** Randomly end user may experience failure to delete object and an error message `you do not have permission to access the request page` pop-up.

**Bug ID:** 110498

**Status:** Fixed in v4.0 MR3.

**Description:** The load balance monitor shows server in IP addresses instead of names and thus it causes unclear when same virtual server point to same real server but different ports.

**Bug ID:** 99595

**Status:** Fixed in v4.0 MR3.

**Description:** VPN monitor may display some abnormal components in IE browser.

**Bug ID:** 124209

**Status:** Fixed in v4.0 MR3.

**Description:** A firewall administrator with `super_read_only` right may fail to backup system configurations.

**Bug ID:** 126414

**Status:** Fixed in v4.0 MR3.

**Description:** A firewall administrator fails to see wireless AP profile if he has only `prof_admin` or `super_read_only` rights.

**Bug ID:** 127194

**Status:** Fixed in v4.0 MR3.

**Description:** The configured alias of a VLAN interface can not be seen on web UI.

**Bug ID:** 130752

**Status:** Fixed in v4.0 MR3.

**Description:** Filter may corrupt on VPN monitor page when thousands IPSec tunnels were on the list.

**Bug ID:** 132042

**Status:** Fixed in v4.0 MR3.

**Description:** Adding widget of Top Sessions may cause NPU interfaces drop connections when FortiGate works in TP mode and traffic volume is extremely high.

**Bug ID:** 132099

**Status:** Fixed in v4.0 MR3.

**Description:** Deleting firewall addresses may be failed via web UI when thousands firewall addresses have been configured.

**Bug ID:** 125134

**Status:** Fixed in v4.0 MR3.

**Description:** The password can be seen on FortiToken details page.

**Bug ID:** 136489

**Status:** Fixed in v4.0 MR3.

## 6.3 System

**Description:** New predefined Radius service does not open UDP port 1645 and 1646 for backward compatibility.

**Bug ID:** 123439

**Status:** Fixed in v4.0 MR3.

**Description:** SMTP daemon process crashes regularly if DLP sensors for spam are enabled but no rule is configured.

**Bug ID:** 126522

**Status:** Fixed in v4.0 MR3.

**Description:** SNMP walk on VPN table takes much longer than expected.

**Bug ID:** 127197

**Status:** Fixed in v4.0 MR3.

**Description:** `npu info` field is needed in debug session list information.

**Bug ID:** 130675

**Status:** Fixed in v4.0 MR3.

**Description:** Default value for auto-backup to FortiManager is set to enable.

**Bug ID:** 131282, 134302

**Status:** Fixed in v4.0 MR3.

**Description:** `proxyworker` `encounter` process may randomly crash.

**Bug ID:** 131869, 131135

**Status:** Fixed in v4.0 MR3.

**Description:** SNMP query with unknown engine ID will be dropped by FortiGate.

**Bug ID:** 130787

**Status:** Fixed in v4.0 MR3.

**Description:** Duplicated firewall services names/address groups may be occurred after upgrade and cause FortiManager failing to retrieve configurations.

**Bug ID:** 135270

**Status:** Fixed in v4.0 MR3.

**Description:** Backup revision of configurations failed to work properly under TP mode.

**Bug ID:** 127040

**Status:** Fixed in v4.0 MR3.

**Description:** Legacy SNMP OID 3.00 shall be removed from MIB tree.

**Bug ID:** 137314

**Status:** Fixed in v4.0 MR3.

**Description:** MTU size of GRE tunnel shall be changed accordingly to the binding physical interface.

**Bug ID:** 135814

**Status:** Fixed in v4.0 MR3.

**Description:** Some of 3G modems may have tiny packets lose due to ALT mode enabled.

**Bug ID:** 125809

**Status:** Fixed in v4.0 MR3.

**Description:** Memory usage kept growing very slowly during daily operation.

**Model Affected:** FortiGate models that support NP4 interfaces

**Bug ID:** 139158

**Status:** Fixed in v4.0 MR3.

**Description:** SNMP statistic is not accurate on XLR interfaces when IPS is enabled and OID is using 32 bit counter.

**Model Affected:** FortiGate models that support XLR card

**Bug ID:** 138680, 139558

**Status:** Fixed in v4.0 MR3.

**Description:** Management IP may not be accessed successfully in TP mode while forward-domain option is enabled in a multi-VLAN environment.

**Bug ID:** 138189

**Status:** Fixed in v4.0 MR3.

## 6.4 High Availability

**Description:** Statistics of some firewall policies may fail to show correct data on new master when failover happened in virtual cluster environment

**Bug ID:** 83105

**Status:** Fixed in v4.0 MR3.

**Description:** Synchronization of configurations may fail partially between master and slave if an admin account is authenticate by a Radius server.

**Bug ID:** 108286, 134100

**Status:** Fixed in v4.0 MR3.

**Description:** Unnecessary logging message are popup by slave when central management is enabled without an IP address assigned.

**Bug ID:** 116730

**Status:** Fixed in v4.0 MR3.

**Description:** Invalid sessions may be created under A-A mode HA cluster environment when traffic volume reach peak level.

**Bug ID:** 124527

**Status:** Fixed in v4.0 MR3.

**Description:** FortiGate may be run into freeze state occasionally under A-P mode HA cluster environment.

**Model Affected:** FortiGate-1240B

**Bug ID:** 123950

**Status:** Fixed in v4.0 MR3.

## 6.5 Router

**Description:** BFD settings in OSPF does not work properly.

**Bug ID:** 135854, 135852

**Status:** Fixed in v4.0 MR3.

**Description:** Reboot of FortiGate may cause RIP lost some configured interfaces when thousands interfaces are enabled in RIP.

**Bug ID:** 139243

**Status:** Fixed in v4.0 MR3.

## 6.6 Firewall

**Description:** A section title may be failed to created when the included VLAN interface has space in its name.

**Bug ID:** 129537

**Status:** Fixed in v4.0 MR3.

**Description:** FSAE\_Guest\_Users group is not available for FSAE explicit proxy authentication configuration under identity based firewall policy.

**Bug ID:** 133933

**Status:** Fixed in v4.0 MR3.

**Description:** Firewall fails to support TCP based DNS query translation and DNS zone transfer translation.

**Bug ID:** 134722

**Status:** Fixed in v4.0 MR3.

**Description:** A Specific group name is not showed in authentication logs when the user belong to multiple groups.

**Bug ID:** 132529

**Status:** Fixed in v4.0 MR3.

**Description:** User that belong to multiple group does not have combined services access.

**Bug ID:** 97872

**Status:** Fixed in v4.0 MR3.

**Description:** Order of Multicast firewall policy can not be adjusted.

**Bug ID:** 131676

**Status:** Fixed in v4.0 MR3.

## 6.7 IPS

**Description:** Configuring service in DoS firewall policy does not behave like expected.

**Bug ID:** 130016

**Status:** Fixed in v4.0 MR3.

## 6.8 VPN

**Description:** SSL VPN tunnel mode users may fail to get result of DNS resolution if they use 64bit windows OS.

**Bug ID:** 115358

**Status:** Fixed in v4.0 MR3.

**Description:** SSL VPN portal FTP client is not compatible with Novell Netware FTP server.

**Bug ID:** 122594

**Status:** Fixed in v4.0 MR3.

**Description:** Using a bookmark to access Novell GroupWise Web Access failed to work properly under SSL VPN web mode.

**Bug ID:** 139028

**Status:** Fixed in v4.0 MR3.

**Description:** Function keys F13-F24 are not supported by Telnet Proxy client in SSL VPN web mode.

**Bug ID:** 125178

**Status:** Fixed in v4.0 MR3.

**Description:** Authentication to internal server may fail when SSO is disabled on SSL VPN portal.

**Bug ID:** 126088

**Status:** Fixed in v4.0 MR3.

**Description:** SSL proxy mistakenly used the CA certificate's *issuer* but not *subject* as the new issuer.

**Bug ID:** 134744, 134412

**Status:** Fixed in v4.0 MR3.

**Description:** SSL VPN daemon failed to release memory when FortiGate enter conserve mode and may cause VPN users connection dropped randomly.

**Bug ID:** 126985, 124068

**Status:** Fixed in v4.0 MR3.

**Description:** SSL VPN monitor failed to work properly under HA virtual cluster environment.

**Bug ID:** 128857

**Status:** Fixed in v4.0 MR3.

**Description:** New issued PIN from RSA Radius server failed to authenticate on FortiGate..

**Bug ID:** 137974

**Status:** Fixed in v4.0 MR3.

**Description:** Copy and paste password does not work for SSL VPN web portal login.

**Bug ID:** 136403

**Status:** Fixed in v4.0 MR3.

**Description:** Firewall local user with LDAP password may fail to login SSL VPN web portal.

**Bug ID:** 130498

**Status:** Fixed in v4.0 MR3.

**Description:** CLI command to change MTU size on a IPSec interface does not take effect.

**Bug ID:** 119523

**Status:** Fixed in v4.0 MR3.

**Description:** Dial-up IPSec VPN between third party device and FortiGate randomly dropped and takes longer to reconnect.

**Bug ID:** 138230

**Status:** Fixed in v4.0 MR3.

**Description:** SAP server access may not work properly in SSL VPN web mode.

**Bug ID:** 115058

**Status:** Fixed in v4.0 MR3.

**Description:** Framed IP address may not be released properly when Radius authentication method is used and PPTP VPN has been disconnected.

**Bug ID:** 138060

**Status:** Fixed in v4.0 MR3.

## 6.9 Web Filter

**Description:** URLfilter process may keep crashing and cause CPU spike when Daily log of remaining quota is enabled.

**Bug ID:** 130152

**Status:** Fixed in v4.0 MR3.

**Description:** Web filter log message does not contain 'Quota Used' and 'Quota Exceeded Info' information when web filter quota is enforced.

**Bug ID:** 124964

**Status:** Fixed in v4.0 MR3.

**Description:** Web filter quota does not take effect on local category after configured.

**Bug ID:** 138266

**Status:** Fixed in v4.0 MR3.

## 6.10 Instant Message

The following IMs and their versions are tested in FortiOS v4.0 MR3.

IM Client	Versions	Comment
AIM	5.9.6089	none
ICQ	7.2.3525	none
Yahoo!Messenger	10.0.0.1270	none
MSN 2009	14.0.8117.416	none

Description: The following table lists the known issues with each of the IMs supported by FortiOS v4.0 MR3.

Models Affected: All

Bug ID: see table

Clients Affected	Versions	Description/Models Affected/Status/BugID
All	All	<b>Description:</b> diag imp2p users all index numbers do not function and may cause crash of imd process. <b>Status:</b> Fixed in v4.0 MR3. <b>Bug ID:</b> 0139324
AIM	5.9.6089	<b>Description:</b> AIM regular file transfer will be canceled by FortiGate. <b>Status:</b> Fixed in v4.0 MR3. <b>Bug ID:</b> 0123629
AIM	5.9.6089	<b>Description:</b> The count of AIM Since Last Reset is reset to 0. <b>Status:</b> Fixed in v4.0 MR3. <b>Bug ID:</b> 0140314
ICQ	7.2.3525	<b>Description:</b> Yahoo's blocking on virus transfer doesn't work properly. <b>Status:</b> Fixed in v4.0 MR3. <b>Bug ID:</b> 0140731

## 6.11 WAN Optimization

**Description:** WAD process randomly crashed in Multi-VDom HA cluster environment.

**Bug ID:** 130580, 132824

**Status:** Fixed in v4.0 MR3.

**Description:** Web cache option was unnecessarily turned on on non-WANOpt models.

**Bug ID:** 138531

**Status:** Fixed in v4.0 MR3.

## 6.12 Log & Report

**Description:** Log\_id of DHCP event log error messages is not compatible with the description in FortiGate Log Message Reference Version 4.0 MR1.

**Bug ID:** 123966

**Status:** Fixed in v4.0 MR3.

**Description:** Host name, file name, file type, file filter type, sent and received bytes information will be added into DLP content archive logs.

**Bug ID:** 130759, 137883, 138860, 138781

**Status:** Fixed in v4.0 MR3.

**Description:** Sent and Received bytes information will be added into Web Filter logs.

**Bug ID:** 137873

**Status:** Fixed in v4.0 MR3.

**Description:** Miglogd process may cause CPU spike when the amount of current sessions reaches certain level.

**Bug ID:** 132703

**Status:** Fixed in v4.0 MR3.

**Description:** Statistics of total discarded logs by Kernel shows via CLI.

**Bug ID:** 135014

**Status:** Fixed in v4.0 MR3.

**Description:** Incompatible DLP archive log quota on web UI and misleading error message need to be corrected.

**Bug ID:** 126991

**Status:** Fixed in v4.0 MR3.

## 6.13 Wi-Fi

**Description:** Wlan interface setting can not be configured via web UI when it is a member of a defined soft-switch interface.

**Bug ID:** 124886

**Status:** Fixed in v4.0 MR3.

**Description:** Wireless client PC can not be authenticated via Radius server when Wlan is a member of a defined soft-switch interface.

**Bug ID:** 119502

**Status:** Fixed in v4.0 MR3.

**Description:** Limitation on how many clients can connect to FortiGate need to be increased.

**Bug ID:** 121150

**Status:** Fixed in v4.0 MR3.



## 7 Known Issues in FortiOS v4.0 MR3

This section lists the known issues of this release, but is NOT a complete list. For enquiries about a particular bug not listed here, contact Customer Support.

### 7.1 Web User Interface

**Description:** Web UI does not take menu-file option into account.

**Bug ID:** 125829

**Status:** To be fixed in a future release.

### 7.2 System

**Description:** Newly created Identify based firewall policy may need short period to take effect if big configurations have applied.

**Bug ID:** 123261

**Status:** To be fixed in a future release.

**Description:** FortiGate may drop connections when AV database update is performed.

**Bug ID:** 123389

**Status:** To be fixed in a future release.

**Description:** Firewall will send multiple authentication requests to Radius/LDAP server if a user to be authenticated matches multiple identify based firewall policies.

**Bug ID:** 126523, 140246

**Status:** To be fixed in a future release.

**Description:** Large file may fail to download completely.

**Bug ID:** 135480

**Status:** To be fixed in a future release.

**Description:** IPS database updates could trigger FortiGate into conserve mode for a few seconds.

**Bug ID:** 139625

**Status:** To be fixed in a future release.

### 7.3 High Availability

**Description:** Sessions could lose during upgrade when IPSec VPN is configured.

**Model Affected:** FortiGate models that support NP2 interfaces

**Bug ID:** 141125

**Status:** To be fixed in a future release.

### 7.4 Firewall

**Description:** A Firefox browser user may be asked to authenticate endlessly if he is linked from a web page without authentication to a web page that is required authentication.

**Bug ID:** 128865

**Status:** To be fixed in a future release.

### 7.5 Web Filter

**Description:** HTTPS URL filtering does not work properly with explicit proxy.

**Bug ID:** 123801

**Status:** To be fixed in a future release.

## 7.6 Antispam

**Description:** ESMTP Mail using BDAT and LAST is not detected.

**Bug ID:** 112717

**Status:** To be fixed in a future release.

## 7.7 VPN

**Description:** Outlook Web Access may not work properly in SSL VPN web mode when browser Firefox is used.

**Bug ID:** 128618

**Status:** To be fixed in a future release.

**Description:** SSLVPN Proxy does not rewrite `window.open` absolute URL option which could cause some URLs inaccessible in SSL VPN Web mode.

**Bug ID:** 134613

**Status:** To be fixed in a future release.

**Description:** MS Office Communicator Web Access mode may fail to be accessed under SSL VPN web mode.

**Bug ID:** 134613

**Status:** To be fixed in a future release.

**Description:** Mapping network drive lost connection intermittently under SSL VPN tunnel mode.

**Bug ID:** 128201

**Status:** To be fixed in a future release.

**Description:** SSL VPN users with PKI enabled failed to login and error message window popup.

**Bug ID:** 141169

**Status:** To be fixed in a future release.

## 7.8 Log & Report

**Description:** Some models may not upload logs to FAMS in real time.

**Bug ID:** 139913

**Status:** To be fixed in a future release.

**Description:** Some models may fail to produce charts in report.

**Bug ID:** 141279

**Status:** To be fixed in a future release.

## 7.9 FSAE Windows DC Agent

**Description:** The Member of group named in Chinese Character failed to authenticate when FSAE is in Advance mode.

**Bug ID:** 129022

**Status:** To be fixed in a future release.

## 7.10 Web Proxy

**Description:** Enabling Web cache may not work with explicit proxy.

**Bug ID:** 140752

**Status:** To be fixed in a future release.

**Description:** `Proxyworker` may hog memory and may cause FortiGate into conserve mode.

**Bug ID:** 141174

**Status:** To be fixed in a future release.

## 8 Image Checksums

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

(End of Release Notes.)