FortiGate® Multi-Threat Security System

Release Notes
v4.0 MR3

01-430-84420-20110818

FORTINET

Table of Contents

Change Log

Date	Change Description
2011-03-18	Initial Release.
2011-03-21	Updated descriptions in Special Notice Section and Upgrade Information Section.
2011-03-24	Removed bug 140752 from Known Issues Section and added bug 139765 and 140988 into Known Issues Section.
2011-03-24	Added WiFi relative descriptions in Special Notice Section and Upgrade Information Section and
2011-03-25	Updated 3G MODEM support information and FortiAnalyzer support information in Section 5.
2011-03-31	Updated descriptions in Upgrade Information Section and added bug 132040 into Resolved Issues Section.
2011-04-01	Move bug 123261, 141169 and 139913 from Known Issue Section to Resolved Issues Section and added bug 140660 into Known Issues Section.
2011-04-04	Added bug 140671 into Known Issues Section and updated new features descriptions in Section 1.
2011-04-07	Updated descriptions in Upgrade Information Section.
2011-05-11	Updated Summary of Enhancements in Section 1.
2011-06-14	Changed 140988 into Resolved Issues Section.
2011-07-07	Updated all information that related to FASE to be FSSO or FSSO (FSAE).
2011-08-18	Updated description and status for bug 139765 in Known Issues Section.

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, FWF-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-5001B, 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.

- "Local In" Policies to and from the FortiGate
- 2-Factor Authentication
- Authentication Group Matching for TACACS+
- Authentication Page Style Improvements
- Captive Portal for WiFi Authentication
- Configurable Global Admin Profiles
- Configuration Object Tagging
- Configuration Restoration via SCP Protocol
- Configuration Rollback feature
- DHCP Address Reservation
- DHCP6
- DiffServ Per Application Filter
- Distributed ARRP (Automatic Radio Resource Provisioning)
- DLP: Document Fingerprinting
- DNS zone transfer and DNS forwarder feature
- Dynamic Profiles
- Endpoint NAC Improvement
- Enhanced Explicit Proxy feature to support Proxy Chaining
- Enhanced Logging
- Enhanced User Authentication
- Enhanced Web Filter Override
- Explicit FTP proxy
- Explicit Proxy Improvements

- Extends Wireless Controller feature support to FortiAP-220A and FortiAP-220B
- Facebook Application Control
- FAMS and FortiAnalyzer Logging Extensions
- File Filter Reorganization
- Firewall Policy Enhancements
- Firewall Schedule Enforcement
- Firewall Session Control Improvements
- Flow-based DLP Support
- Flow-based Web Content Filtering
- FMC-XG2 Module Support
- FortiASIC Traffic Offload Improvements
- FortiGate Default Report Generation and Improvements
- FTPS protocol support for SSL Inspection
- Geography-based Filtering
- Hosted NAT traversal for RTP pin-holing
- HTTP Host Load Balancing
- Improved Chart Display
- Improved Dashboard Widgets
- Internet Content Adaptation Protocol (ICAP)
- Inter-Product Secure Communications
- Integration of ping-server configurations and improvements
- IPS One-arm on XLR
- IPS Sensor Enhancements
- IPS Signature Search and IPS Signature Threshold
- IPSec 'get' Command Improvement
- IPv6 Firewall Authentication
- IPv6 Firewall Offload on ASM-CE4, ADM-XE2, ADM-FE8 and FMC-XG2 modules
- IPv6 SNMP Support
- Log Viewer Filters
- Merge UTM Logs into one Category
- Modem Interface Improvements
- Monitoring Dynamic Data on FMG
- Monitoring Section in Menu System
- Multicast IGMP Static Join and PIM Enhancement
- Network Scan feature Improvements
- NTLM Authentication Extensions
- Password Renewal for LDAP Users over SSLVPN
- Per-IP Traffic Shaping for Application Control
- Per-VDom Configuration Files
- Per-zone option for Local DNS Server
- Pictures in Replacement Messages
- PKI Authentication Extensions
- Policy Table Web UI Improvements
- 'Port Pair' feature in Transparent mode
- Protocol Identification Tag for FDN Reporting on AV
- Proxy Support with SSL Offload
- Quotas for Web Cache / Byte Cache
- RADIUS Accounting Extension
- Replacement Message Reorganization
- Report Editing Simplification and Improvements
- Rogue AP Detection & Reporting & Suppression
- Session Table Enhancements
- Setup Wizard for FOS

- SHA-384 and SHA-512 Support to IKE and IPsec
- Simple FortiClient VPN GUI
- Simplify Email Filtering
- SNMP Enhancements including web UI support for SNMPv3
- SQL Logging Enhancements
- SSL Proxy: Verify Host SSL Certificates
- SSL-VPN Client in Port Forward mode
- SSL-VPN Policy DE-Authentication
- SSL-VPN Tunnel Widget Improvements
- SSL-VPN Web Mode over IPv6
- Static Route web UI Improvements
- Sub-second Failover for NP4 Ports
- 'Top Session widget' Supports IPv6 sessions
- Traffic Logging Improvements
- Troubleshooting Improvements
- Unified AV Engine
- VRRP Virtual MAC Support
- Web Filter Category Reorganization & Disclaimers & Improvements
- Web UI Consolidation and Enhancements
- Weighted HA Failover Improvements
- WiFi Enterprise Authentication Support

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 Logging to FortiAnalyzer

FortiOS v4.0 MR3 introduces an encrypted communication option between the FortiAnalyzer device and the FortiGate device. Both sides must be running v4.0 MR3. Upgrading a FortiGate device from v4.0 MR2 to MR3 disables the option and ensures the communication between the FortiAnalzyer device and FortiGate device is unaffected. However, loading the FortiOS firmware image using the TFTP boot method enables the encryption option and thus may affect the communication. To disable encrypted communication, use the following CLI command:

```
config log fortianalyzer setting
    set enc-algorithm disable
end
```

2.3 Rename FSAE to FSSO

FSAE has been renamed FSSO—Fortinet Single Sign On. All web UI and CLI objects have been updated.

2.4 Rename WLAN to WiFi

WLAN has been renamed WiFi. All web UI and CLI objects have been updated.

2.5 WiFi Radio Settings

FortiOS v4.0 MR3 has enhanced several areas related to the WiFi feature such as wireless AP profile. As such, wireless radio settings except SSID, Security Mode, Authentication settings are lost after upgrade. The settings must be added after upgrade:

- Create a new Custom AP profile using the web UI
  `WiFi Controller > Managed Access Points > Custom AP Profile > Create`
  Create a new AP profile matching the platform and configuration with the other wireless settings.

- Associate the new AP profile to a Local WiFi Radio
  `WiFi Controller > Managed Access Points > Local WiFi Radio`
  Associate the new AP profile in the wireless settings.

3 Upgrade Information

3.1 Upgrading from FortiOS v4.0 MR2

FortiOS v4.0 MR3 officially supports upgrade from the FortiOS v4.0 MR2 Patch Release 4 or later. See the upgrade path below.

[FortiOS v4.0 MR2]
The upgrade is supported from FortiOS v4.0 MR2 Patch Release 4 B0313 or later.

v4.0 MR2 Patch Release 4 B0313 (or later)
↓
v4.0 MR3 B0441 GA

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

[Web filter overrides]
The contents of web filter overrides will be lost after upgrading from FortiOS v4.0 MR2 Patch Release 4 B0313 to FortiOS v4.0 MR3 B0441.

[AMC slot settings]
The default value of `ips-weight` under `config system amc-slot` will be changed from `balanced` to `less-fw` after upgrading to FortiOS v4.0 MR3.

[Firewall policy settings]
If the source interface or destination interface set as `amc-XXX` interface, the default value of ips-sensor under `config firewall policy` will changed from `all_default` to `default` after upgrading to FortiOS v4.0 MR3.

[Wireless radio settings]
wireless radio settings except SSID, Security Mode, Authentication settings will be lost after upgrade. Workaround is put into Special Notice Section.

3.2 Upgrading from FortiOS v4.0 MR1

FortiOS v4.0 MR3 officially supports upgrade from the FortiOS v4.0 MR1 Patch Release 9 or later. See the upgrade path below.

[FortiOS v4.0 MR1]
The upgrade is supported from FortiOS v4.0 MR1 Patch Release 4 B0213 Patch Release 9 or later.

v4.0 MR1 Patch Release 9 B0213 (or later)
↓
v4.0 MR3 B0441 GA

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

[Network Interface Configuration]
If a network interface has `ips-sniffer-mode` option set to enable, and that interface is being used by a firewall policy, then after upgrading from FortiOS v4.0.0 or any subsequent patch to FortiOS v4.0 MR3 the `ips-sniffer-mode` setting will be changed to `disable`.

[Traffic shaping]

The Unit of `guaranteed-bandwidth`, `inbandwidth`, `outbandwidth` and `maximum-bandwidth` of traffic shaping has been changed from `kilo-bytes/sec` to `kilo-bits/sec` after upgrading to FortiOS v4.0 MR3.

[IPS DoS sensor log setting]
The default log setting of an IPS DoS sensor is `disable` on FortiOS v4.0 MR3. Whether the log stetting of an IPS DoS sensor is `disable` or `enable` on FortiOS v4.1.9 or any subsequent patch, after upgrading to FortiOS v4.0 MR3, the setting will be set to `disable`.

[IPS sensor log setting]
The log setting of IPS sensors is `enable` by default on FortiOS v4.0 MR3. If the log setting of an IPS sensor is disabled on FortiOS v4.1.9 or any subsequent patch, the value will be kept after upgrading to FortiOS v4.0 MR3. If the log setting of an IPS sensor is `enable` or `default` on FortiOS v4.1.9 or any subsequent patch, the value will be changed to `enable` after upgrading to FortiOS v4.0 MR3.

[DLP Rule]
A DLP rule with sub-protocol setting set to `sip simple sccp` will be lost upon upgrading to FortiOS v4.0 MR3.

[System Autoupdate Settings]
The default values of `config system autoupdate schedule` will be changed from `disable` to `enable` after upgrading to FortiOS v4.0 MR3.

[Web filter & spam filter]
The name `webfilter-status` and `spamfilter-status` have been change to `webfilter-force-off` and `antispam-force-off`. The default values is set to `enable` after upgrading to FortiOS v4.0 MR3. To use web filter and spam filter, users have to disable the two entries by using the following CLI command:

```
config system fortiguard
    set webfilter-force-off disable
    set antispam-force-off disable
end
```

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 MR3.

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 FortiAP Support

FortiOS v4.0 MR3 supports the following FortiAP models:

- FortiAP-210B
- FortiAP-220A
- FortiAP-220B

The FortiAP devices must be running FortiAP v4.0 MR3.

5.5 Fortinet Single Sign On (FSSO) Support

FortiOS v4.0 MR3 is supported by FSSO v3.00 B066 (FSSO 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.

5.6 AV Engine and IPS Engine Support

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

5.7 3G MODEM Support

FortiOS v4.0 MR3 has added a new feature whereby a list is downloaded to the FortiGate device from FortiGuard. The download from FortiGuard must be initiated by the administrator – it is not automatic such as AV or IPS push updates. To view the list of supported 3G MODEMs via Web UI, execute the following CLI command:

```
config system modem
    set status enable
end
```

Then user can go to `System > Network > Modem` and click on '`Configure Modem`' on right side. A list of the supported modems is displayed. As well, an "`Update Now`" button at the top can be used to retrieve an updated list of support MODEMS.

5.8 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-621B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW
Internal Hard Drive (FSM-064)	FGT-200B FGT-311B FGT-1240B FGT-3040B FGT-3140B FGT-3951B
Single Width 4-port 1Gbps Ethernet interface (ASM-FB4)	FGT-310B FGT-311B FGT-620B FGT-621B 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-621B FGT-1240B FGT-3016B FGT-3600A

AMC Modules	FortiGate Support
	FGT-3810A FGT-5001A-SW
Single Width 4-port Ethernet bypass interface (ASM-CX4)	FGT-310B FGT-311B FGT-620B FGT-621B 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
AMC Security Processing Engine Module (ADM-XD4)	FGT-3810A FGT-5001A-DW
AMC Security Processing Engine Module (ADM-FE8)	FGT-3810A
Rear Transition Module (RTM-XD2)	FGT-5001A-DW
Four Port T1/E1 WAN Security Processing Module (ASM-ET4)	FGT-310B FGT-311B
Rear Transition Module (RTM-XB2)	FGT-5001A-DW
Fortinet Mezzanine Card (FMC-XG2)	FGT-3950B FGT-3951B FGT-3140B
Fortinet Mezzanine Card (FMC-XD2)	FGT-3950B FGT-3951B

5.9 SSL-VPN Support

5.9.1 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		

5.9.2 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

5.10 SSL-VPN Host Compatibility List

The following Antivirus and Firewall client software packages are supported.

Product	Antivirus	Firewall
Windows XP		
Symantec Endpoint Protection v11	√	√
Kaspersky Antivirus 2009	√	X
McAfee Security Center v8.1	√	√
Trend Micro Internet Security Pro	√	√
F-Secure Internet Security 2009	√	√

Product	Antivirus	Firewall
Windows 7 (32bit)		
CA Internet Security Suite Plus Software	√	√
AVG Internet Security 2011	X	X
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	√	√

Product	Antivirus	Firewall
Windows 7 (64bit)		
CA Internet Security Suite Plus Software	√	√
AVG Internet Security 2011	X	X
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	√	√

5.11 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

5.12 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: It causes confusion on load balance monitor page when multiple virtual servers point to same real server but different ports in load balance configuration.
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.

Description: A new Identity-based firewall policy may need short period to take effect if the configuration is large.
Bug ID: 123261
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 messages are pop up by slave when central management is enabled without an IP address.
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 freeze occasionally on an A-P mode cluster.
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: A copied and pasted 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.

Description: SSL-VPN users with PKI enabled may fail to login in certain instances. When this occurs an error message may be displayed in the web UI.
Bug ID: 141169
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	**Description:**`diag imp2p users all` index numbers do not function and may cause crash of `imd` process. **Status:** Fixed in v4.0 MR3. **Bug ID:**0139324
AIM	5.9.6089	**Description:** AIM regular file transfer will be canceled by FortiGate. **Status:** Fixed in v4.0 MR3. **Bug ID:**0123629
AIM	5.9.6089	**Description:** The count of AIM Since Last Reset is reset to 0. **Status:** Fixed in v4.0 MR3. **Bug ID:**0140314
ICQ	7.2.3525	**Description:** Yahoo's blocking on virus transfer doesn't work properly.

		Status: Fixed in v4.0 MR3. **Bug ID:**0140731

6.11 Voice Over IP (VoIP)

Description: SIP calls may fail to be transferred due to early UPDATE packets were dropped.
Bug ID: 132040
Status: Fixed in v4.0 MR3.

6.12 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.

6.13 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.

Description: A FortiGate device may fail to upload logs to FAMS in real time.
Bug ID: 139913
Status: Fixed in v4.0 MR3.

6.14 WiFi

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 may clients can connect to FortiGate need to be increased.
Bug ID: 121150
Status: Fixed in v4.0 MR3.

Description: Upgrade to 4.3 will be failed if WLAN interface is a member of soft-switch.
Bug ID: 140988, 140512, 140893
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.

Description: VLAN interfaces fail to appear on network page in specific VDom if VLAN interface and its binding physical interface do not belong to the same VDom.
Bug ID: 140671
Status: To be fixed in a future release.

7.2 System

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.

Description: `Proxyworker` may hog memory and may cause FortiGate into conserve mode.
Bug ID: 141174
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 Antispam

Description: ESMTP Mail using BDAT and LAST is not detected.
Bug ID: 112717
Status: To be fixed in a future release.

7.6 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: 134620
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.

7.7 Log & Report

Description: Some models may fail to produce charts in report.
Bug ID: 141279
Status: To be fixed in a future release.

Description: '`logtraffic-app`' option is disabled by default when a new firewall policy is created via Web UI.
Bug ID: 140660
Workaround: Use the CLI command "`config firewall policy>edit #>set logtraffic-app enable`" to enable it.
Status: To be fixed in a future release.

7.8 FSSO (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.

7.9 WiFi

Description: FortiWiFi-80CM and FortiWiFi-81CM devices that use the RT2880 WiFi chipset are not supported by FOS v4.0 MR3.
Bug ID: 139765
Model Affected: FortiWiFi-80CM and and FortiWiFi-81CM devices that use the RT2880 WiFi chipset..
Status: Due to hardware limitation this issue will not be fixed.

7.10 Web Proxy

Description: HTTPS URL filtering does not work properly with explicit proxy.
Bug ID: 123801
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.)