FORTINET
High Performance Network Security

FortiManager - Release Notes

VERSION 5.4.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 08, 2018

FortiManager - Release Notes

02-543-416486-20180608

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-05-18	Initial release of 5.4.3.
2017-05-23	Added 433623 and 424321 to Known Issues.
2017-05-29	Updated *FortiGuard Distribution Servers (FDS)*.
2017-06-01	Added *Compatibility with FortiOS Versions > Compatibility issues with FortiOS 5.4.5* and *Product Integration & Support > 5.4.5*.
2017-06-05	Moved 356454 from *Resolved Issues > Known Issues*.
2017-06-08	Added *Compatibility with FortiOS Versions > Compatibility issues with FortiOS 5.4.5*
2017-06-19	Added *Product Integration and Support > Virtualization > ESXi 6.5*.
2017-06-22	Added 404368 to *Resolved Issues > Policy & Objects*.
2017-06-27	Added 401234 to *Resolved Issues > System Settings*.
2017-08-21	Added 380790 to *Known Issues > Others*.
2017-08-24	Removed FG-7040E-8 and FG-7060E-8 from *Product Integration & Support > FortiGate Models (5.4)*.
2017-08-30	Updated bug 416486 description in *Known Issues > Device Manager* section.
2017-09-01	Updated *Product Integration & Support > Web Browsers*. Added 416840 to *Known Issues > Others*. Removed *Management Features* support from *Product Integration & Support > Feature Support > FortiSandbox.* Added *Reports* support to *Product Integration & Support > Feature Support > FortiSandbox.*
2017-09-06	Updated FortiOS support in *Product Integration and Support*.
2017-09-27	Updated *Product Integration & Support > Feature Support > FortiAnalyzer > added Reports and Logging*.
2017-12-05	Added 407044 to *Resolved Issues > Global ADOM*.
2018-02-21	Added information about upgrading from 5.2.x.

Date	Change Description
2018-06-08	Added 458908 to *Known Issues* > *Others*.

Introduction

This document provides the following information for FortiManager 5.4.3 build 1187:

- Supported models
- Special Notices
- Upgrade Information
- Product Integration and Support
- Compatibility with FortiOS Versions
- Resolved Issues
- Known Issues
- FortiGuard Distribution Servers (FDS)

For more information on upgrading your device, see the FortiManager *Upgrade Guide*.

Supported models

FortiManager version 5.4.3 supports the following models:

FortiManager	FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV (including Hyper-V 2016), FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).

What’s new in FortiManager 5.4.3

The following is a list of new features and enhancements in 5.4.3. For details, see the *FortiManager Administrator Guide*:

Not all features/enhancements listed below are supported on all models

FortiMeter Update

FortiOS VM resourced based metering program is now available. The license model is based on the CPU and memory usage. In this update, more granular service offerings, such as FW+1 Service, FW+2 Services, FW+3 Services and FW +UTM, are provided. It supports up to four interfaces and two VDOMs.

FortiWebOS-VM traffic volume and service type based metering program is also available.

Central DNAT per policy package support

You can create a new DNAT entry from the Central DNAT page of a policy package by creating a new virtual IP or using an existing virtual IP. The newly created virtual IP object from the DNAT entry is saved to the *DNAT and Virtual IPs* table and is shared amongst different policy packages.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.4.3.

FortiGate VM 16/32/UL license support

FortiOS 5.4.4 introduces new VM license types to support additional vCPUs. FortiManager 5.4.3 supports these new licenses with the prefixes of FGVM16, FGVM32, and FGVMUL.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

IPsec connection to FortiOS for logging

FortiManager 5.4.2 with FortiAnalyzer Features enabled no longer supports an IPsec connection with FortiOS 5.0.x/5.2.x. However UDP or TCP + reliable are supported.

Instead of IPsec, you can use the FortiOS reliable logging feature to encrypt logs and send them to FortiManager. You can enable the reliable logging feature on FortiOS by using the `configure log fortianalyzer setting` command. You can also control the encryption method on FortiOS by using the `set enc-algorithm default/high/low/disable` command.

FortiManager 5.4.1 and earlier supports IPsec connection with FortiOS 5.0.x/5.2.x.

VM License (VM-10K-UG) Support

FortiManager 5.4.2 introduces a new VM license (VM-10K-UG) that supports 10,000 devices. It is recommended to upgrade to FortiManager 5.4.2 before applying the new license to avoid benign GUI issues.

If you use the new license with FortiManager 5.4.1 or 5.2.x and earlier, the maximum number of devices is correctly enforced, but the GUI may display some VM information incorrectly. For example, the VM storage maximum may incorrectly display 100GB in the *License Information* widget on the *System Settings* pane. The VM license type may not appear (FortiManager 5.4.1), and the VM license type may show *Unknown* (FortiManager 5.2.9).

System Configuration or VM License is Lost after Upgrade

When upgrading FortiManager from 5.4.0 or 5.4.1 to 5.4.2, it is imperative to reboot the unit before installing the 5.4.2 firmware image. Please see the *FortiManager Upgrade Guide* for details about upgrading. Otherwise, FortiManager may lose system configuration or VM license after upgrade. There are two options to recover the FortiManager unit:

1. Reconfigure the system configuration or add VM license via CLI with `execute add-vm-license <vm license>`.
2. Restore the 5.4.0 backup and upgrade to 5.4.2.

FortiOS 5.4.0 Support

With the enhancement in password encryption, FortiManager 5.4.2 no longer supports FortiOS 5.4.0. Please upgrade FortiGate to 5.4.2.

The following ADOM versions are not affected: 5.0 and 5.2.

Local in-policy after upgrade

After upgrading to FortiManager 5.4.1, you must import or reconfigure local in-policy entries. Otherwise, the subsequent install of policy packages to FortiGate will purge the local in-policy entries on FortiGate.

ADOM for FortiGate 4.3 Devices

FortiManager 5.4 no longer supports FortiGate 4.3 devices. FortiManager cannot manage the devices after the upgrade. To continue managing those devices, please upgrade all FortiGate 4.3 to a supported version, retrieve the latest configuration from the devices, and move the devices to an ADOM database with the corresponding version.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
   set ssl-protocol t1sv1
end
```

Upgrade Information

Upgrading to FortiManager 5.4.3

You can upgrade FortiManager 5.2.0 or later directly to 5.4.3. If you are upgrading from versions earlier than 5.2.0, you will need to upgrade to FortiManager 5.2 first. (We recommend that you upgrade to 5.2.9, the latest version of FortiManager 5.2.)

Bug ID	Description
404193	ADOM upgrade will fail if the MGMT interface is a dedicated management port and mapped to a dynamic interface. **Workaround**: Before upgrading to 5.4, you should remove MGMT interface from dynamic interface zone, if a managed FortiGate has MGMT interface and if it is a dedicated management port. This is because MGMT interface being set to a dedicated management port cannot be mapped to a dynamic interface zone in 5.4.

For details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

During upgrade from 5.2.4 or earlier, invalid dynamic mappings and duplicate package settings are removed from the ADOM database. Please allow sufficient time for the upgrade to complete.

Upgrading from 5.2.x

Starting with FortiManager 5.4.0, you can create a maximum number of Global and ADOM objects for each object category, and the maximum is enforced. The maximum numbers are high and unlikely to be met. The purpose of the maximum is to help avoid excessive database sizes, which can impact performance.

During upgrade from FortiManager 5.2.x to 5.4.x to 5.6.2, objects are preserved, even if the 5.2 ADOM contains more than the maximum number of allowed objects. If you have met the maximum number of allowed objects, you cannot add additional objects after upgrading to FortiManager 5.6.2.

Following are examples of object limits:

- Firewall service custom: 8192 objects
- Firewall service group: 2000 objects

If you have reached the maximum number of allowed objects, you can reduce the number of objects by deleting duplicate or obsolete objects from the ADOM.

You can also reach the maximum number of allowed objects if you have multiple FortiGate/VDOMs in the same ADOM.

You can reduce the number of objects by moving the FortiGates/VDOMs into different ADOMs.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

FortiManager 5.4.3 support

The following table lists 5.4.3 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects. • Mozilla Firefox version 53 • Google Chrome version 58 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier	• 5.4.5 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.5, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.4 on page 26. • 5.4.4 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.4, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.4 on page 26. • 5.4.1 to 5.4.3 • 5.2.8 to 5.2.11 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.10 on page 26. • 5.2.7 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.7 on page 27. • 5.2.6 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.6 on page 27. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.1 on page 27. • 5.2.0 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility issues with FortiOS 5.2.0 on page 27. • 5.0.4 to 5.0.14 FortiManager 5.4.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.14, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.0.4 on page 28.

FortiAnalyzer	• 5.4.0 to 5.4.3 • 5.2.0 to 5.2.11 • 5.0.0 to 5.0.13
FortiCache	• 4.2.2 • 4.1.2 • 4.0.0 to 4.0.4
FortiClient	• 5.4.3 • 5.4.1 • 5.2.0 and later
FortiMail	• 5.3.7 to 5.3.9 • 5.2.9 • 5.1.6 • 5.0.10
FortiSandbox	• 2.3.2 • 2.2.1 • 2.1.2 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.2.3 • 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.8.0 • 5.6.0 • 5.5.4 • 5.4.1 • 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6

FortiDDoS	• 4.3.1 • 4.4.2 • 4.2.3 • 4.1.11 Limited support. For more information, see Feature support on page 17.
FortiAuthenticator	• 4.3.2
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 6.2 • Linux KVM Redhat 6.5 • Microsoft Azure • Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2 • OpenSource XenServer 4.2.5 • VMware • ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0 and 6.5

To confirm that a device model or firmware version is supported by current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiCache			✓	✓

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
FortiAuthenticator				✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
```

```
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiManager CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 5.4.3.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE,FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-2000E, FG-2500E, FG 3800D **FortiGate 5000 Series:** FG-5001C, FG-5001D **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC **FortiGate Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-30D-POE, FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE, FWF-92D, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, o FG-VM64-AZUREONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600D, FG-900D, FG-600C, FG-620B, FG-621B, FG-800C, FG-800D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM-Azure, FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-700D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:**FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.0

FortiCarrier Models

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3800D-DC, FCR-3810D-DC, FCR-3815D-DC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND	5.2
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.0

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1.6
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0.10

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.3.2
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.0
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-2000E	5.6.0
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.3

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.8
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E **FortiCache VM:** FCH-VM64, ForiCache-KVM	4.1
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64	4.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E, FAC-VM	4.0 and 4.1

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.4.3.

Compatibility issues with FortiOS 5.4.5

The following table lists interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS 5.4.5.

Bug ID	Description
434637	FortiGate `config ssd-trim-freq` causes FortiManager retrieval failure.
417581	AP Profile in AP Manager missing AP Country Code for TZ (Tanzania).

Compatibility issues with FortiOS 5.4.4

The following table lists interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS 5.4.4.

Bug ID	Description
407566	The *accesspoint-name* of an extended controller is lost when name contains more than thirty one characters.
407577	FortiManager should support the following syntax: `gui-domain-ip-reputation` and `auth-multi-group`.
407579	FortiManager should support the CLI, `ipsec-dec-subengine-mask`, on platforms that equip with the NP6 chipset.

Compatibility issues with FortiOS 5.2.10

The following table lists interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS 5.2.10.

Bug ID	Description
397220	FortiOS 5.2.10 increased the maximum number of the firewall schedule objects for 1U and 2U+ appliances. As a result, a retrieve may fail if more than the maximum objects are configured.

Compatibility issues with FortiOS 5.2.7

The following table lists interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS 5.2.7.

Bug ID	Description
365757	Retrieve may fail on LDAP User Group if object filter has more than 511 characters.
365766	Retrieve may fail when there are more than 50 portals within a VDOM.
365782	Install may fail on system global optimize or system fips-cc entropy-token.

Compatibility issues with FortiOS 5.2.6

The following table lists interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS 5.2.6.

Bug ID	Description
308294	1) New default wtp-profile settings on FOS 5.2.6 cause verification errors during installation. 2) FortiManager only supports 10,000 firewall addresses while FortiOS 5.2.6 supports 20,000 firewall addresses.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS version 5.2.1.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263896	If it contains the certificate: `Fortinet_CA_SSLProxy` or `Fortinet_SSLProxy`, `retrieve` may not work as expected.

Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS version 5.2.0.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Compatibility issues with FortiOS 5.0.5

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.1 and FortiOS version 5.0.5.

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Compatibility issues with FortiOS 5.0.4

The following table lists known interoperability issues that have been identified with FortiManager version 5.4.3 and FortiOS version 5.0.4.

Bug ID	Description
226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
226078	When the password length is increased to 128 characters, the installation fails.
226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.
226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS 5.0.5.
226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Resolved Issues

The following issues have been fixed in 5.4.3. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
305734	The folder list in import wizard may not be in alphabetical order.
372709	Timeout of network errors may occur when creating a chassis.
373580	Dashboard may be displayed in both management and non-management VDOMs.
390931	If a phase1-interface is monitored by another, it may need to be purged twice to remove this interface.
393629	When users clone a static route, the device entry may not be displayed on GUI.
394294	The same routing table may be displayed for different VDOMs.
395173	Deleting 100 devices may cause a dvm lock.
397520	After FortiManager upgrades, it may incorrectly install np6 session-collector-interval 8 to 5.2.4 FortiGates.
401844	FortiAnalyzer settings may be missing in CLI-Only object.
401845	DNS settings may be missing in CLI-Only object.
402005	Some E series FortiGates may have incorrect `config "logdisk=0"`.
404083	If two static routes share the same gateway, the one without internet-service may get deleted during installation.
404470	Users may fail to upgrade low-end FortiGates from FortiManager.
405082	Integrity check of policy package may always include policy ippool check even had the ippool of the VDOM set to be disabled.
405227	Installation may hang if an interface has "Default Mapping" enabled with the value being NULL.

Bug ID	Description
408927	Static routes with named address on the same interface may get deleted upon installation to FortiGates.
411195	Importing a device db revision may fail.
412145	Users may not be able to add an NTP server by DNS name in provisioning Template.
412158	FortiManager may accept any for Interface-passive.
416792	FortiGate may display the HA status as up when it is in standalone mode.

Global ADOM

Bug ID	Description
421979	Assigning a global policy package may not work as expected.
407044	Autobackup causes `system global` to have two entries.

Policy and Objects

Bug ID	Description
274882	Subnet mask with notation of /x style may cause installation to fail.
281820	FortiManager may not support central-snat-map creation from GUI.
357026	The override link may not be displayed if the blocked FortiGuard categories are pushed from FortiManager.
379128	Drop-down list of security profile may always be empty list and with loading indicator spinning.
379191	Users may not be able to select a URL address as the destination address from the Explicit Proxy Policy in the GUI.
393641	Importing policy to one device may cause another device policy package status to become modified, if they share the dynamic parent interface with each other.
396422	Users may not be able to search for *Address Objects* with CIDR notation in the Policy View.

Bug ID	Description
400354	Deleting a global policy package assignment may not remove the global policies assigned to the ADOM.
400844	After upgrade from 5.2.4, policy package may fail to set associated-interface of firewall address.
401366	After FortiManager upgrades to 5.4.2, editing a security profile directly from the Policy view may cause various visual problems.
401369	Install policy package may fail if copying a switch-interface with a VAP interface.
401475, 401476	After FortiManager upgrades to 5.4.2, viewing IP Pools in GUI takes long time to load, which may result in viewing invisible.
401481	Changes for web categories and addresses under SSL exemption in SSL/SSH profiles may not be saved in GUI.
401485	Policy installation to nested groups may not work.
402112	FortiManager may not create an attack_id automatically for custom IPS signature without an attack_id.
402138	Quarantine action in right-click menu for a signature in IPS profile may not work.
402261	Duplicate Dynamic Mappings are created if some VIP objects in a VIP group reference a Zone Interface.
404368	`ippool overlap` copy error occurs if you change the name of an installed ip pool.
404895	Install policy package may fail if a dynamic VIP is bonded to an interface, which also has dynamic mappings.
404971	The GUI may show an empty dynamic mappings list after editing the mappings.
405425	Policy Package installation to FortiGates may fail if it includes a VIP that has been renamed recently.
405430	Installation may hang if there is a large list of AD groups.
408027	There might be security console crashes if some address groups have empty members.
408436	The action *Reset* may not be displayed for *Application Control* in FortiManager GUI.
409025	Reordering static urlfilter may not work.
410727	Invalid global policies may be copied to ADOMs during assignment and cannot be deleted.
410776	A cloned object may not have the same group membership as the original one.

Bug ID	Description
411337	Action Proxy is missing for tcp_syn_flood under DoS policies in GUI.
411650	The URL table ID may also be cloned when a web filter profile is cloned.
412591	Where used may not work for 5.0 ADOMs.
412848	Policy table view may only accept 35 characters at the maximum for comments.
415296	Comments for IP Pools may not be shown in the list page.
415391	Changing a firewall address type from IP range value to IP subnet value may cause the installation to fail.
416315	`fwpolicy-implicit-log` may be unset after a global policy package has been assigned to an ADOM policy package.
416530	Some object groups may not be able to be added to an installation target of a specific policy.
416813	*Policy Import* may fail due to the failure to create mappings for VPN SSL web portal.
417229	APNs may not be displayed in the GTP profiles.
422780	VIP Groups with dynamic mappings may not install.
808439	Users may not be able to enter Policy and Objects page if the ADOM has been locked and unlocked at the same time by different users.

Revision History

Bug ID	Description
400344	FortiManager may accept characters for `session-ttl`, causing an installation to fail.

Script

Bug ID	Description
401474	Running scripts on Nested Groups may fail.
404065	TCL scripts with “clock” may not work.

Bug ID	Description
404269	The "unselect member" option may not work.
405769	Install concurrent script may fail when deploying it on large number of devices.
406655	Scheduled CLI script to run on remote device may be run on device database instead.
411964	In the Device Selection page, if you search for a new key word, the previous selection may be lost.
411975	Running a script against a group may fail.

Services

Bug ID	Description
404787	Users may not be able to view and configure web proxy under FortiGuard Web Filter and Email Filter Settings.
411205	Using the command `execute fmupdate ftp import custom-url` may skip some invalid URLs in the file.

System Settings

Bug ID	Description
364775	The Log Receive Monitor widget may show Device ID instead of Device Name.
396417	Mail server connection test from GUI may fail.
398324	Power online/offline events or SNMP traps may not be generated.
407916	The *Save* button may not be triggered when policy section title is changed under workspace mode.
411262	Users may not be able to create a session when its device manager privilege is ReadOnly.
401234	Unable to enable/disable administrative service on the VLAN interface.

VPN Manager

Bug ID	Description
383176	Installation may hang if configuring VPN by creating dynamic IPSec Zone.
397946	It may not be able to display SSL VPN settings in VPN Manager.
400869	Copying VPN configuration may fail by specifying randomly generated pre-shared keys.
401424	VPN central management ADOM may fail to upgrade from v5.2 to v5.4 due to invalid dynamic mappings.
404909	After FortiManager upgrade 5.4.2, zones and dial-up tunnels may be removed when installing policy package.
405240	Users may not be able to create multiple IPSec VPN Phase 1’s on a same interface.
407997	SSL VPN Monitor may not work.
408165	After removing a gateway from the VPN console, if the users try to add it back, there will be a duplicate gateway error during installation.
413684	Creating an IPSec VPN Phase 1 with option to Create FortiClient VPN may fail.
417580	Deleting a gateway from the VPN topology may not remove IPsec Phase 1 and its related tunnels.
422730	Installation may fail if an address group is used in the protected subnet in the VPN.

AP Manager

Bug ID	Description
286686	When Wifi template specifies a security mode requiring RADIUS, authentication of Radius does not come up as expected.
400116	Users may not be able to assign wtp profile for Local-WiFi if the platform's local wifi is pre-fixed with 'FW' not 'FWF'.
401921	FortiManager may not be able to configure a FortiWiFi correctly regarding to setting the maximum number of Access Points that the FortiWiFi could support.
401983	User may not be able to configure a long-shared secret for a radius server with auth_type is PAP.
407822	Users may not be able to configure User Groups and the Exempt List for SSID profiles.

Others

Bug ID	Description
376022	The alert *HA cluster is down.* may be shown, even if the cluster is back up again.
397863	The `execute fmscript list` command may return the incorrect ADOM for a script.
399646	Auto-update of FortiManager accidentally changes its HA mode from SLBC to standalone, which results in losing connection between FortiManager and SLBC.
401251	ADOM upgrade may fail because of the `wtp-profile`.
401924	FortiAnalyzer VM on Microsoft Azure may combine the temporary disk and new inserted data disk into one single logical volume used for log storage when executing `execute lvm start`.
405409	XML request `addPmConfig54AdomObjFirewallServiceCustom` may not accept the dash inside port ranges.
405789	When there is no device, `diagnose pm2 check-integrity` may report an error.
407889	The command `execute dmserver showconfig` may display some JSON output before configurations.
409731	SNMP trap may not be sent when the interface is up.
410373	SATA and SCSI driver may not be supported on KVM platforms.
413568	SNMP query for `ifInOctets/ifOutOctets` may return `counter64` instead of `counter32`.

Common Vulnerabilities and Exposures

Bug ID	Description
401614	FortiManager 5.4.3 is no longer vulnerable to the following CVE-Reference: • 2012-6704 Visit https://fortiguard.com/psirt for more information.
402095	FortiManager 5.4.3 is no longer vulnerable to the following CVE-Reference: • 2016-10009 Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
404282	FortiManager 5.4.3 is no longer vulnerable to the following CVE-Reference: • 2017-3126 Visit https://fortiguard.com/psirt for more information.
405125	FortiManager 5.4.3 is no longer vulnerable to the following CVE-References: • 2017-3731 • 2017-3730 • 2017-3732 • 2016-7055 Visit https://fortiguard.com/psirt for more information.
405226	Policy Package name accepts malicious content which can cause XSS attack.
408241	FortiManager 5.4.3 is no longer vulnerable to the following CVE-References: • 2016-5766 • 2016-6132 • 2016-6207 • 2016-6128 • 2016-5767 • 2015-8874 • 2016-9317 • 2016-6912 • 2016-10166 • 2016-10167 • 2016-10168 Visit https://fortiguard.com/psirt for more information.
416917	FortiManager 5.4.3 is no longer vulnerable to the following CVE-References: • 2016-10229 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.4.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
395156	Changing SSID configuration of AP profile may not trigger `configuration-install`.

Device Manager

Bug ID	Description
401746	FortiManager may set the license of web filter to expired on FortiGate 5001D blades in SLBC/ELBC chassis setup.

Policy & Objects

Bug ID	Description
403564	FortiManager may not be able to install an object when `partial-install` is on.
433623	The policy interface pair view may not pair properly; duplication may occur. **Workaround**: Use the policy column filter function to view by interface pair.

VPN

Bug ID	Description
356454	SSL VPN monitor may show information for VDOMs managed by other ADOMs.
424321	After creating a new VPN Community and moving a device to new a VPN, the copy installation may not work because the device has the old VPN configuration. **Workaround**: Remove the VPN Community `device db config` first. For example, after removing the device from the previous VPN Community, do an install first.

Others

Bug ID	Description
374711	Following an ADOM upgrade from 4.3 to 5.0, policies with invalid objects may be removed. **Workaround**: Remove interface binding from invalid objects before ADOM upgrade.
380790	Linefeed code in PAC File for ExplictProxy my change from *CR LF* to *LF*.
401014	Apache being down intermittently may block access to GUI through HTTP or HTTPs. **Workaround**: Change the port-number of HTTP and of HTTPS temporarily to other port-number.
416840	Microsoft Internet Explorer or Edge may not completely render a page with a large set of policies or objects. **Workaround**: Please use Mozilla Firefox or Google Chrome to view the page
458908	`devid` in `dvmdb/device` is displayed as a Hostname.

FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	• 5.0.0 and later • 5.2.0 and later • 5.4.0 and later • 5.6.0 and later	✓		✓	
FortiClient (Windows)	• 4.3.0 and later	✓			
FortiClient (Windows)	• 4.2.0 and later	✓	✓		✓
FortiClient (Mac OS X)	• 5.0.1 and later • 5.2.0 and later	✓		✓	
FortiMail	• 4.2.0 and later • 4.3.0 and later • 5.0.0 and later • 5.1.0 and later • 5.2.0 and later • 5.3.7 to 5.3.9	✓	✓		

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later • 2.1.2 • 2.2.1 • 2.3.2	✓			
FortiWeb	• 5.0.6 • 5.1.4 • 5.2.0 and later • 5.3.0 • 5.4.1 • 5.5.4 • 5.6.0 • 5.8.0	✓			

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
   set status enable
end
```

High Performance Network Security