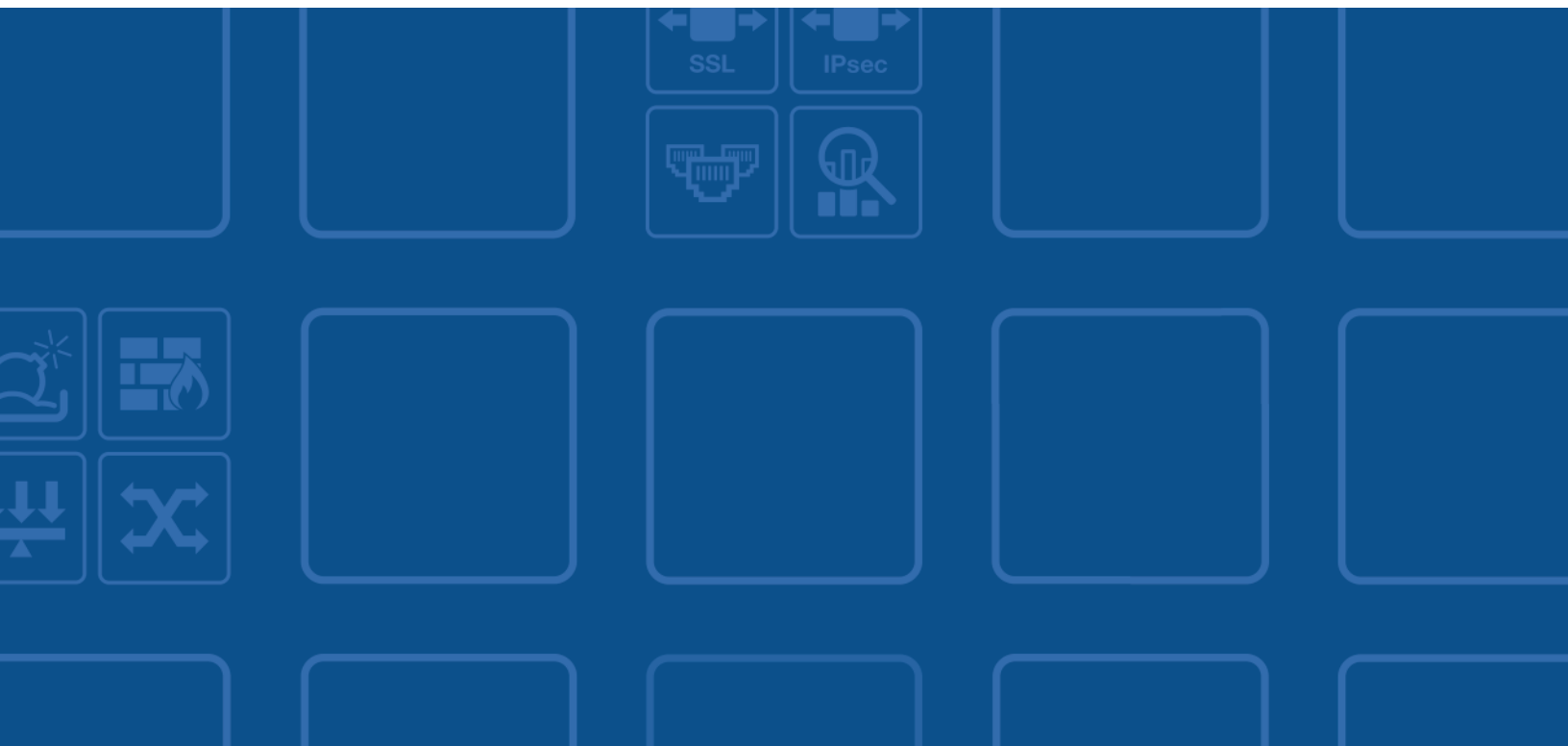
FORTINET
High Performance Network Security

FortiManager - Release Notes

VERSION 5.4.2



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

July 7, 2018

FortiManager - Release Notes

02-542-393534-20180711

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-12-14	Initial release of 5.4.2.
2016-12-15	Added 400068 to Known Issues and 383563 to Resolved Issues. Removed 390355 from Resolved Issues and updated 389255 in Resolved Issues. Noted that FortiManager supports Microsoft Hyper-V 2016 in the FortiManager VM Firmware section. Updated FortiGuard Center Update Support section to include FortiClient 5.4.0 and later.
2016-12-20	Removed 378367 from the Compatibility with FortiOS Versions section.
2016-12-21	Added support for FortiOS 5.4.3 and updated the following special notice: System Configuration or VM License is Lost after Upgrade.
2016-12-22	Added 400869 to Known Issues.
2016-12-29	Added special notice about Hyper-V FortiManager-VM running on an AMD CPU.
2017-01-03	Added 401366 to Known Issues.
2017-01-06	Added 382001 to Resolved Issues.
2017-01-09	Updated CVE number for 382001 in Resolved Issues.
2017-01-27	Added 404895 to Known Issues.
2017-02-23	Added support for FortiOS 5.4.4.
2017-04-25	Added 404470 to Known Issues.
2017-06-01	Added support for FortiMail 5.3.8.
2017-09-01	Clarified FortiSandbox support in Feature support on page 16.
2018-02-21	Added information about upgrading from 5.2.x.
2018-07-11	Added 376839 to Resolved Issues.

Introduction

This document provides the following information for FortiManager 5.4.2 build 1151:

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

Supported models

FortiManager version 5.4.2 supports the following models:

FortiManager	FMG-200D, FMG-300D, FMG-300E, FMG-400E, 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 5.4.2

The following is a list of new features and enhancements in 5.4.2. For details, see the *FortiManager Administrator Guide*:

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

Policy Search and Filtering

The *Column Filter* option is now available from the *Search* box. You add filters from the search box or from the contextual menu by right-clicking an object entry.

Admin Profile Granularity

Additional options are available to help granular control of administrative access privileges. The new options include:

- Licensing, Firmware Management and Advanced for FortiGuard Center
- Revert Configuration from Revision History for Device Manager
- Interface Mapping for Policy & Objects

Automatically Promote Device with Pre-shared Key

Automatically promote a model device to a managed device by using a pre-shared secret.

First you add the model device to FortiManager by using a pre-shared key. When the device connects to FortiManager, run the `execute central-mgmt register-device <FMGSN> <KEY>` command from the FortiGate's console. The device is now automatically promoted, and the configuration of the matched model device is applied.

For FortiOS 5.4.1 or earlier, you must run the `execute central-mgmt register-device <FMGSN> <KEY> <username> <password>` command.

Package Management Usability

Improved the information display for FortiGuard Package Management.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.4.2.

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 5.4.2

You can upgrade FortiManager 5.2.0 or later directly to 5.4.2. 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.)

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 5.4.2 support

The following table lists 5.4.2 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11.0 • Mozilla Firefox version 50 • Google Chrome version 54 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier	• 5.4.4 FortiManager 5.4.2 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 25. • 5.4.1 to 5.4.3 • 5.2.8 to 5.2.10 FortiManager 5.4.2 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 25. • 5.2.7 FortiManager 5.4.2 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 25. • 5.2.6 FortiManager 5.4.2 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 26. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.4.2 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 26. • 5.2.0 FortiManager 5.4.2 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 26. • 5.0.4 to 5.0.14 FortiManager 5.4.2 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 27.
FortiAnalyzer	• 5.4.0 to 5.4.2 • 5.2.0 to 5.2.9 • 5.0.0 to 5.0.13

FortiCache	• 4.1.2 • 4.0.0 to 4.0.4
FortiClient	• 5.4.1 • 5.2.0 and later
FortiMail	• 5.3.8 • 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	• 5.6.0 • 5.5.4 • 5.4.1 • 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6
FortiDDoS	• 4.4.2 • 4.2.3 • 4.1.11 Limited support. For more information, see Feature support on page 16.

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, and 6.0

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			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiWeb		✓	✓	✓
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 5.4.2.

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-90D, FG-90D-POE,FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, 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, 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-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-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 5.4.2.

Compatibility issues with FortiOS 5.4.4

The following table lists interoperability issues that have been identified with FortiManager version 5.4.2 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 5.4.2 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 5.4.2 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.

Bug ID	Description
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 5.4.2 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 5.4.2 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 5.4.2 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 5.4.2 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 5.4.2. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
363354	Changing policy route configurations directly on FortiGate with a retrieve may change the policy package status to “Unknown”.
366436	Users may not be able to change admin password for FortiGate from FortiManager if the password has expired on FortiGate.
373645	Certificates generated from Certificate Template and VDOM may have the same DN.
374612	Moving a device to backup ADOM may cause FortiGate HA cluster to become Out-of-Sync.
376426	Changing any value in Webfilter FortiGuard settings may change the over-auth-port-http and over-auto-port-https range to 0-5.
377259	Adding a FortiGate may fail if the device is also added as an unregistered device during the process.
378070	If users try to use custom NTP server in Provisioning Templates, FortiManager may wrongly try to setup the ntpserver key.
378239	Upgrading an ADOM from 5.2 to 5.4 may unset FortiAnalyzer log settings and FortiGuard settings in Provisioning Templates.
378273	Users adding widgets on a FortiGate may cause the configuration status to be Out-of-Sync.
378580	Users may not be able to create or edit conditional-advertisement for BGP neighbor from GUI.
378759	Policy Package status may not be changed to “Modified” following a deletion of a URL Filter entry.
382044	Routing policies may not be moved.
384122	Policy package status remains modified after installation or import when hit count feature is enabled.

Bug ID	Description
385514	Users may not be able to select a specific VDOM to generate a certificate form a certificate template.
385700	Model device may always have the same version as the ADOM version.
386290	The tooltips in License page may not work.
389127	System template may not be assigned to more than ten devices.
374708	The disclaimer page limit for replacement message is different from that on FortiGate.
376042	Users may not be able to schedule an upgrade in device dashboard.
385498	FortiManager may not be able to upgrade multiple FortiAP devices at once from GUI.
386235	A restricted admin who manages a list of VDOMs with changes may not be able to install to FortiGate.
389163	Users may need to refresh first before cloning a newly created static route.
392446	Users may not be able to delete a system template with an empty name.
394499	After upgrade, FortiManager may not show any devices under *Managed FortiGate*.
366726	Users may not be able to change FortiGate HA device sequence for FortiOS 5.2.7.
391458	Users may not be able to create a provisioning template from device if the SNMP community host has been assigned an interface.
394664	FortiManager may not correctly convert IP mask for static route's destination.
394853	FortiManager may not be able to install device settings after `set md5-key` is set under `configure ospf-interface`.
395476	Users may not be able to add more than one user group to SSID template.
302371	Installation may fail when FortiManager tries to set built-in certificate's password.

Global ADOM

Bug ID	Description
378822	Users may not be able to un-assign ADOM from a global ADOM policy package.
391247	Users may not be able to use a virtual-wan-link interface for global policies.

Policy and Objects

Bug ID	Description
289205	Users may not see or set status for custom IPS signatures from FortiManager.
290751	Users may not be able to add a local-in-policy.
296592	The search results may not contain firewall service objects with searched value within port ranges.
302616	Within an address object, users may not be able to see the assigned group.
306134	Users may not be able to drag and drop an object between columns.
360610	“Where used” may not show correct results.
363970	Users may not be able to open result of “Policy Consistency Check”.
374622	Modifying an interface may create a second dynamic mapping for the same interface.
376357	For Virtual IP range, the upper IP range may have smaller valve than the lower IP range.
377913	The configuration, “tertiary-secret,” of a radius server may not be installed to FortiGate.
379249	The policy order may be incorrect in section view after inserting or cloning a policy.
379252	Section View collapsed section may expand again after policy change.
379260	GUI may not retain the selection option for section view.
379267	Users may not be able to go back to “where used” result page after editing a policy in the result.
379274	Users may not be able to view nested groups.
379919	Searching for a string in Application Control may contain results for searching as substring.
379948	GUI may not display dynamic objects with special characters.
379955	Tags may not be visible in a policy.
380336	The ordering for IDs may be correct when users select section view.
380449	FortiManager may not support more than ten Fortinet Single Sign-on Agent objects.
380457	When users add new members to FSSO groups, FortiManager may prompt an unresponsive script error.

Bug ID	Description
381460	Users may not be able to close the inline editing box on the policy summary page.
382950	Under workflow mode, Revision Diffs between sessions may not show the changes.
383079	Changing application control profile, which is within a profile group, does not trigger policy package status to change.
385696	Policy package name may be missing in install wizard.
386013	FortiManager cannot set block on Proxy.HTTP application in explicit proxy policy.
386682	Policy package names in install wizard may not be listed in alphabetical order.
386738	Users may not be able to configure Advanced Options within a VoIP security profile.
386768	Users may not be able to edit an object with its name containing a trailing '\t' character.
388591	FortiManager may not be able to import FortiGate configurations when there is an AD group having apostrophe in its name.
388850	Group membership changes done at object level may not be applied.
390367	Web Rating Overrides may show numeric value instead of symbolic category name.
391259	When re-importing a device, FortiManager should not change fsso-polling objects if fsso-polling IDs have not changed.
278434	The *authtimeout* setting may be missing under *Advanced Options* within *User Group* object.
357026	The override link may not be displayed if the blocked FortiGuard categories are pushed from FortiManager.
370645	FSSO may not be automatically enabled when users drag an FSSO group into the authentication field.
370983	Users may not be able to view *local-in-policy* and *local-in-policy6* from GUI under a policy package.
378548	Advanced settings of Virtual IP objects may not be installed to FortiGate devices.
382993	DNS filter may not be imported to FortiManager.
385456	In the *FSSO object* configuration page, the *Refresh & Apply* button may remove entries from remote LDAP servers.
386159	The option to configure Traffic shaping may not be shown in GUI after users edit an application control profile.

Bug ID	Description
386444	*Reverse Traffic Shaping* may not be visible if users disabled *Traffic Shaping*.
389177	Users may not be able to use a Virtual IP object as destination address in *Explicit Web Proxy Policy*.
391604	Users may not be able to see dynamic mappings for an object under *Object Configuration*.
391620	The *configure default value* checkbox may be missing from GUI when users create a new Virtual IP object.
392443	Installation may fail if there are quarantine-expiry changes on rate-based IPS signatures.
394478	Users may see cached information when editing a profile group if they have edited one before.
357429	Where used may not work for Local Categories.
397336	Edit page for User Group may display incorrect group members.
394088	If `device-identification` is enabled for an interface, FSSO settings may be purged during policy installation.

Revision History

Bug ID	Description
295540	After upgrade, FortiManager may purge report layout during Policy Package install.
301077	FortiManager may install outdated CRL to FortiGate.
310915	FortiManager may configure invalid IP settings for modem interface.
367113	Rename an IP pool may cause the installation to fail.
369743	The ha-priority setting may cause installation to fail.
377941	A long protocol-profile name may lead to installation failure.
378564	FortiManager cannot install FortiClient endpoint profile related configurations to FortiGate-500D.
379134	Installation may fail if users set portmapping for Virtual IP.
381890	The ordering of the configurations may be incorrect for identity based explicit web proxy policy with NTLM.

Bug ID	Description
382146	When users create a service with FQDN, the “set iprange” may be used instead of “set fqdn”.
383176	Policy installation may get stuck at 67% before installation preview.
384878	FortiManager may not be able to install wildcard admin account to FortiGate.
385268	Setting override configurations for FortiAnalyzer may result in an installation error.
385924	Installation to v5.2.5 FortiGate may fail because of wireless-controller wtp-profile.

Script

Bug ID	Description
385902	Config status may be changed to Modified if no changes are made to the database after executing a script.
388531	Script execution history may show unencrypted password of a FortiGate admin.
387885	There is a possibility that script task may hang.
391057	Users may not be able to run a script if Workspace Normal mode is enabled.

Services

Bug ID	Description
368449	No warning may be given if the users have decreased the service level for a FortiGate within FortiMeter.
374556	FortiManager may not display FortiAP images’ model names on the FortiGuard Firmware Images page.
381536	AV PUSH updates may not get snet to FortiMail.
385925	Users may not be able to disable TLSv1 for FortiGuard services.
386414	The status of a FortiGate license may be affected by Mobile Malware status.
391905	FortiManager may not be able to upgrade the firmware on some FortiGate models.

System Settings

Bug ID	Description
296680	Device registration may fail due to SSL Fragmentation on TCP port 541.
354410	A jsonconsole session may be counted in as an admin session even if it has been disconnected.
370121	FortiManager may not show “Receive an update package from FDS” in Event logs.
375319	Read-only admins may not be able to view difference between two revisions.
375728	Users may not be able to delete an ADOM if it belongs to a script group.
379044	Event logs may not log information about Sync Status, Device Settings Status, and Policy Package status.
380072	The downloaded Event logs may contain some unwanted HTML codes.
384357	Unsupported ADOM version may exist.
386334	There may not be a “Back” button within the Historical Log page.
387226	Emails generated from workflow may not work if Email Authentication is not enabled.
387246	In Workflow mode, FortiManager may not be able to send Emails via startttls with a secured SMTP server.
388275	The lengths of some SNMP fields may not be RFC compliant.
391022	End of Daylight Savings time zone for Turkey/Istanbul GMT +3.
392342	FortiManager may not prevent the browser from showing previous login names.
354410	The `jsconsole` sessions may still be counted in the admin session list when the sessions no longer exist
375204	Wildcard admin with *user_type* set to *group* may not be able to login via GUI.
393480	For Two Factor Authentication admins, hitting *Enter* key from keyboard may not be perceived as Login attempt.

VPN Manager

Bug ID	Description
375256	VPN IPSec phase 1 may not support the new DPD configuration options: on-demand and on-idle.
384628	XAUTH and User Group options disappear when IP Assignment Mode is Range or IKE Configuration Method is disabled.
386080	If VPN console uses custom zone with mappings, there may be crash or copy fail during installation validation stage.
386902	Searching for a device may not work in VPN Manager.
387573	FortiManager may not allow the same PeerID or LocalId within IPSec Phase1 interface.
306430	Dynamic mapping for address may not be supported for VPN phase 2.
388021	Users may not be able to re-import policies with VPN enabled system zones.
394719	Users may be able to enable `auto-negotiate` and `keep-alive` at the same time and thus it may cause the installation to fail.
393104	Users may not be able to specify *any* interface under SSL-VPN settings.

Others

Bug ID	Description
281126	JSON API response may contain unencrypted password.
305468	FortiManager may not display a message when the maximum number of login sessions has been reached.
366726	Users may not be able to change the FortiGate HA device sequence for FortiGate HA clusters.
371814	It may take more than two minutes to get a response for 3000 policies with JSON APIs.
373376	The CLI command, “execute fmpolicy copy-adom-object,” may not work.
375575	FortiManager may lose its configuration during upgrade if the /tmp folder is full.
377244	HA may not be able to establish when FortiManager has many large databases.

Bug ID	Description
377727	FortiManager should allow users to delete portal users.
378447	FortiView may not work after FortiManager upgrades from 5.4.0.
378579	The attributes, wifi-key and wifi-password, should not be required when users create an interface using JSON APIs.
379088	The “set endpoint-compliance enable” may be missing in the interface configuration.
379078	The fgfmsd daemon may consume 100% CPU resources.
380619	The command, “diagnose dvm device list”, may not generate a complete device list if the database is corrupted.
381461	FortiManager may not support xterm-256color terminal.
382790	Users may not be able to create a loopback interface via JSON APIs.
388071	FortiAnalyzer may not be able to render a proper web GUI page when making a change.
366033	GUI may not display all ADOM revisions.
393295	The command `diagnose cdb check adom-integrity` may modify `ALL_ICMP` service object.
396074	After running the `diagnose cdb check adom-integrity` command, FortiManager may install an empty policy package to FortiGate if workspace mode is enabled.
396595	Some check-integrity commands may modify database when the ADOM is locked.
376839	VULN: SSH, Cipher acrfourxxx was reported as vulnerability in nessus scan.

Common Vulnerabilities and Exposures

Bug ID	Description
309902	FortiManager 5.4.2 is no longer vulnerable to the following CVE-Reference: • 2016-3193 Visit https://fortiguard.com/psirt for more information.
380634	FortiManager 5.4.2 is no longer vulnerable to the following CVE-Reference: • 2016-5387 Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
383809	FortiManager 5.4.2 is no longer vulnerable to the following TMP-Reference: • 2016-0023 Visit https://fortiguard.com/psirt for more information.
389255	FortiManager 5.4.2 is no longer vulnerable to the following CVE-References: • 2016-6304 • 2016-6305 • 2016-2183 • 2016-6303 • 2016-6302 • 2016-2182 • 2016-2177 • 2016-2178 • 2016-2179 • 2016-2181 • 2016-6306 • 2016-6307 • 2016-6308 Visit https://fortiguard.com/psirt for more information.
389615	FortiManager 5.4.2 is no longer vulnerable to the following CVE-References: • 2016-6309 • 2016-7052 Visit https://fortiguard.com/psirt for more information.
380634	FortiManager 5.4.2 is no longer vulnerable to the following CVE-Reference: • 2016-5387 Visit https://fortiguard.com/psirt for more information.
383563	FortiManager 5.4.2 is no longer vulnerable to the following CVE-Reference: • 2016-5696 Visit https://fortiguard.com/psirt for more information.
382001	FortiManager 5.4.2 is no longer vulnerable to the following CVE-Reference: • 2016-8495 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.4.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
305187	Device Manager may display the same policy package name for VDOMs with different policy packages installed.
397342	Users may not be able to change the encryption option or disable WiFi broadcast setting in AP Manager.

Policy & Objects

Bug ID	Description
399877	Install DNS Filter profile failed for category. **Workaround**: Perform the configuration changes by using *Policy & Objects* > *Object Configurations* > *CLI Only Objects* > *dnsfilter profile* and *waf profile*.
399837	DNS Filter profile add new *Domain Filter* not saved . **Workaround**: Perform the configuration changes by using *Policy & Objects* > *Object Configurations* > *CLI Only Objects* > *dnsfilter profile* and *waf profile*.
399870	Install WAF profile failed for *constraint exception*. **Workaround**: Perform the configuration changes by using *Policy & Objects* > *Object Configurations* > *CLI Only Objects* > *dnsfilter profile* and *waf profile*.
400026	Policy table, view log by policy UUID does not work due to missing UUID in *Log View*.
400068	If VIP configured interface is *any*, create new policy or edit policy, and if policy incoming interface is not *any*, cannot select that VIP from object selection list. **Workaround**: When policy source interface is *any*, select *any* interface VIP, and then change to another interface. Alternately, you can run a script to generate the configuration, or you can change VIP configured interface to be the same as incoming interface.
401366	Edit Security Profile configuration by using the Policy Package policy list on the right side of the pane, and Object Selection pane shows incorrect configuration page. **Workaround**: Edit configuration from Object Configuration - Security Profiles list.

Bug ID	Description
404895	Install policy package may fail if a dynamic VIP is bonded to an interface, which also has dynamic mappings. **Workaround**: When defining a dynamic VIP, use *ANY* as the bonding interface.

Script

Bug ID	Description
391674	Users may not be able to change snmp-index via a script.
397863	The command, “execute fmscript list”, may return scripts from different ADOMs.

VPN

Bug ID	Description
382045	SL VPN portal changes may not be installed to FortiGate.
400869	Copy VPN configure fails, if using randomly generated pre-shared key. **Workaround**: Change to Specify Pre-Shared Key, or change to Specify Pre-Shared Key first, save, and then change to certificate authentication.

Others

Bug ID	Description
374711	If there is an invalid object in a policy, the policy package may lose all the policies after upgrade. **Workaround**: Remove the invalid object before upgrade.
383227	Adding a FortiGate to a backup ADOM may incorrectly set the device running in normal mode.
392623	FortiManager slave may stop receiving FortiGate logs after FortiGate’s device name has changed.
404470	Users may fail to upgrade low-end FortiGates from FortiManager.

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	✓		✓	
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	✓	✓		
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later	✓			

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiWeb	• 5.0.6 • 5.1.4 • 5.2.0 and later • 5.3.0	✓			

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
```

FORTINET®

High Performance Network Security