High Performance Network Security

FortiManager - Release Notes

VERSION 5.4.0

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

February 21, 2018

FortiManager - Release Notes

02-540-301377-20180221

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-02-17	Initial release.
2016-02-18	Corrected FortiGate and FortiClient supported models.
2016-02-19	Updated FortiManager 5.4.0 support information; added Known Issue 310570.
2016-02-24	Updated language support; added ADOM support to Special Notices.
2016-03-31	Added support for FortiOS/FortiOS Carrier 5.2.7 and compatibility issues.
2016-04-26	Added 307847 to Resolved Issues.
2016-05-25	Added FAZ-400E for version 5.4 to Supported Models.
2016-06-22	Added FAZ-1000E for version 5.4 to Supported Models.
2016-07-12	Made minor correction of FortiManager 5.4.0 support for FortiOS/FortiOS Carrier.
2016-12-29	Added special notice about Hyper-V FortiManager-VM running on an AMD CPU.
2018-02-21	Added information about upgrading from 5.2.x.

Introduction

This document provides the following information for FortiManager 5.4.0 build 1019:

- Supported models
- What’s new in FortiManager 5.4.0
- 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 5.4.0 supports the following models:

FortiManager	FMG-200D, FMG-300D, FMG-300E, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMG-VM64-KVM, FMG-VM64-AWS, and FMG-VM64-HV.

What’s new in FortiManager 5.4.0

The following is a list of new features and enhancements in 5.4.0. For details, see *FortiManager Administrator Guide*.

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

- Address, Service, and Schedule used objects deletion
- Integrated FortiGuard License Management page in GUI
- ADOM exclusions for Administrator
- Centralized SSL-VPN management
- VPN management usability improvements
- Unique policy names
- Unmapped zone improvements

- Revision Control Extensions
- Handling of Installation Error improvements
- Sort ADOM list by Mode
- Option to find Duplicated Objects
- Policy Hit Count support
- Support Management of FSSO User/Group at the ADOM level
- New WebUI Navigation when ADOM is Enabled
- WAN Link Load Balance Manager
- Pay-as-you-go License Server
- FortiClient Endpoint Manager
- Responsive flat GUI

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.4.0.

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.

ADOM Upgrade for FortiManager 5.4

Upgrade is available for ADOM version 5.0 to migrate to version 5.2. Currently, there is no ADOM upgrade option for ADOM version 5.2 to move to version 5.4.

Monitors and Queries with FortiOS 5.4.0

The following monitors and queries on FortiManager require installing a dedicated FortiOS 5.4.0 build:

- FortiClient Monitor
- FortiAP Monitor
- VPN Monitor
- Policy Hit Count
- All Query functions on Device Manager

Please contact Fortinet Customer Support to download the dedicated build.

Multicast Policy Support at ADOM Level

Starting from FortiManager 5.2.2, configuration for multicast policy has been moved from individual FortiGate devices to an ADOM database. For FortiManager units that are upgraded from a previous release, all multicast policies must be imported into the ADOM database or reconfigured manually. Otherwise, the FortiManager will delete all existing multicast policies on the FortiGate when installing a policy package.

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
```

SQL database rebuild

Upgrading the device firmware can trigger an SQL database rebuild. During this time, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Web Portal support

Web Portal is no longer available as it has been replaced by Restricted Admin Profile. Users can still access web portal content via the Web Portal API services.

CLI commands for configuring dynamic objects

All dynamic objects are consolidated from devices to the ADOM database. For those users who wish to configure a dynamic mapping via a CLI script, the configuration for the mapping must be defined in the dynamic object under the `config dynamic_mapping` sub-tree. Also, the CLI script must be run on policy package instead of the device database. Below are some examples:

Example 1: Dynamic VIP

```
config firewall vip
  edit "vip1"
  …
  config dynamic_mapping
    edit "FW60CA3911000089"-"root"
      set extintf "any"
      set extip 172.18.26.100
      set mappedip 192.168.3.100
      set arp-reply disable
    next
  end
end
```

Example 2: Dynamic Address

```
config firewall address
   edit "address1"
   …
   config dynamic_mapping
      edit "FW60CA3911000089"-"root"
         set subnet 192.168.4.0 255.255.255.0
      next
   end
end
```

Example 3: Dynamic Interface

```
config dynamic interface
…
   config dynamic_mapping
      edit "FW60CA3911000089"-"root"
         set local-intf internal
         set intrazone-deny disable
      next
   end
end
```

FortiManager VM

In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider before installing or upgrading FortiManager VM.

FortiAnalyzer feature set

In version 5.2.0 or later, the FortiAnalyzer feature set (FortiView, Event Management, and Reports) is disabled by default. To enable the FortiAnalyzer feature set, enter the following CLI commands:

```
config system global
   set faz-status enable
end
Changing faz status will affect FAZ feature in FMG. If you continue, system will reboot
    to add/remove FAZ feature.
Do you want to continue? (y/n)
```

Enter `y` to continue, your device will reboot with the FortiAnalyzer features enabled.

In version 5.4.0, you can enable the FortiAnalyzer feature set in the Web-based Manager. Go to *System Settings* > *Dashboard*. In the *System Information* widget, beside *FortiAnalyzer Features*, select *Enabled*.

FortiGate firmware upgrade

After completing a FortiGate firmware upgrade via FortiManager, you must manually retrieve the device configuration.

System time on FortiManager VM

If an NTP server is not reachable from a FortiManager VM unit, it will use the VMware ESX/ESXi host's time as the system time.

Memory requirement for FortiManager VM64-HV

A minimum of 2GB of memory is required to normally operate FortiManager VM64-HV for Microsoft Hyper-V environments.

ADOM for FortiCarrier

Please note that FortiGate and FortiCarrier devices can no longer be grouped into the same ADOM in FortiManager. FortiCarrier devices should be grouped into a dedicated FortiCarrier ADOM.

After upgrade, FortiCarrier devices will no longer be shown in any of the existing ADOMs. When creating a FortiCarrier ADOM, the FortiCarrier devices will be listed and can be grouped into the ADOM.

ADOM mode must be enabled in order to create a FortiCarrier ADOM and manage FortiCarrier devices.

FortiOS 5.0 override server setting for FortiGuard Services

FortiOS no longer has the option to specify an IP address or a domain name for FortiGuard services. FortiGate either connects to the FortiGuard Distribution Network (FDN) or the managing FortiManager for update services. If a FortiGate is required to retrieve updates from a specific FortiManager or FortiGuard server, please use port address translation (PAT) to redirect update traffic to the proper IP address and port.

This is applicable to FortiOS version 5.0 devices only. FortiOS version 5.2 has a different behavior.

Ports used by FortiGuard services

Port	Service
8890	Antivirus or IPS updates for FortiGate
53 or 8888	Web Filtering or Antispam queries for FortiGate
8891	Antivirus or IPS updates for FortiClient
80	Web Filtering or Antispam queries for FortiClient

The public FDN uses port 443 to provide antivirus/IPS updates. In FortiManager, it uses port 8890 (FortiGate) / port 8891 (FortiClient) instead. See the two examples below.

Example 1: Antivirus/IPS

In this example, the FortiGate (10.1.100.1) is managed by FortiManager1 (172.16.200.102) and gets antivirus/IPS updates from FortiManager2 (172.16.200.207). A NAT/PAT device (10.1.100.2/172.16.200.2) sits between the FortiGate and the FortiManager.

In the FortiGate, enter the following CLI commands to enable FortiManager FDS override and set the FortiManager IP address (internal IP on NAT/PAT device):

```
config system central-management
   set fortimanager-fds-override enable
   set fmg "10.1.100.2"
end
```

On the NAT/PAT device, configure the following IP and port translations:

```
10.1.100.2:8890 -> 172.16.200.207:8890
10.1.100.2:541 -> 172.16.200.102:541
```

Example 2: Web filtering/Antispam

In this example, the FortiGate (10.1.100.1) is managed by FortiManager1 (172.16.200.102) and performs web filtering and antispam queries on FortiManager2 (172.16.200.207). A NAT/PAT device (10.1.100.2/172.16.200.2) sits between the FortiGate and the FortiManager.

On the FortiGate, enter the following CLI commands to enable FortiManager FDS override and set the FortiManager IP address (internal IP on NAT/PAT device):

```
config system central-management
   set fortimanager-fds-override enable
   set fmg "10.1.100.2"
end
```

On the NAT/PAT device, configure the following IP and port translations:

```
10.1.100.2:53/8888 -> 172.16.200.207:53/8888
10.1.100.2:541 -> 172.16.200.102:541
```

Update services provided to FortiMail 4.2 devices

Please enable the following option in order to provide update services to FortiMail version 4.2 devices:

```
config fmupdate support-pre-fgt43
   set status enable
end
```

Endpoint management

In version 5.0 and later, FortiClient endpoint agent configuration and management are now handled by the FortiGate Endpoint Control feature. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. This feature requires a FortiGate device running FortiOS version 5.0.0 or later.

For more information, see the *Device and Client Reputation for FortiOS Handbook* available at http://docs.fortinet.com.

FortiManager VM license check

As part of the license validation process, FortiManager compares its IP addresses with the IP information in the license file. If the IP addresses do not match, FortiManager returns the error `IP does not match` as part of the CLI command `get system status` output. If a new license has been imported or the FortiManager's IP address has been changed, the FortiManager will reboot itself for the system to validate the change and operate with a valid license.

Multi-language display support

FortiManager has restrictions on supporting the multi-language display of a FortiGate device.

Importing a FortiManager generated policy

FortiManager has the option to import all policies from a FortiGate device into a single policy package. Due to design limitations, the import process removes all policies with FortiManager generated policy IDs, such as 1073741825, that previously were learned by a FortiManager unit. The FortiGate unit may inherit a policy ID from:

- Global Header Policy
- Global Footer Policy
- VPN Console

Importing profile group and RADIUS dynamic start server

Please be advised that the *Import Wizard* does not import profile group and RADIUS dynamic start server objects which are not referenced by firewall policies. Please configure those objects on your FortiManager device.

Push update in bi-directional static NAT

Whenever there is a NAT device between FortiGate devices and the FortiManager with bi-directional static NAT enabled, you must follow the instructions below in order for FortiGate devices to receive *Push Update* announcements from the FortiManager.

Configure the following settings on FortiManager:

```
config fmupdate av-ips push-override-to-client
   set status enable
   config announce-ip
      edit 1
         set ip <the override IP that the FortiGate uses to download updates from the
             FortiManager>
         set port <the port that the FortiManager uses to send the update announcement>
      end
   end
end
```

Upgrade Information

Upgrading to FortiManager 5.4.0

You can upgrade FortiManager 5.2.0 or later directly to 5.4.0. 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 5.2.4, the latest version of FortiManager 5.2).

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

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, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Microsoft Hyper-V Server

- `.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.

VMware ESX/ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 32-bit or 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/virtual-security-management.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 5.4.0 support

The following table lists 5.4.0 product integration and support information:

Web Browsers	• Microsoft Internet Explorer 11.0 • Mozilla Firefox version 42 • Google Chrome version 47 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 5.4.0 • 5.2.0 to 5.2.7 FortiManager 5.4.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0 to 5.2.7, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 27. • 5.0.4 to 5.0.12 FortiManager 5.4.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.12, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 27.
FortiAnalyzer	• 5.4.0 • 5.2.0 to 5.2.5 • 5.0.0 to 5.0.11
FortiCache	• 3.1.1 • 3.0.0 to 3.0.4
FortiClient	• 5.4.0 • 5.2.0 and later
FortiMail	• 5.3.1 • 5.2.6 • 5.1.5 • 5.0.8

FortiSandbox	• 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	• 5.5.1 • 5.4.0 • 5.3.7 • 5.2.4 • 5.1.4 • 5.0.6
FortiDDoS	• 4.1.11
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 6.2 • Linux KVM Redhat 6.5 • 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		✓		✓
FortiMail		✓	✓	✓
FortiSandbox	✓	✓		✓
FortiSwitch ATCA	✓			
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, 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 5.4.0.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-50E, FG-51E, FG-60D, FG-60D-POE, FG-70D, FG-70D-POE, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-140D, FG-140D-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FGT-280D-POE, FGT-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C,FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D **FortiGate 5000 Series:** FG-5001C, FG-5001D **FortiGate DC:** FG-600C-DC, FG-800C-DC, FG-1000C-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810D-DC **FortiGate Low Encryption:** FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30E, FWF-50E, FWF-51E, FWF-30D-POE, FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiGate Rugged:** 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-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-3700DX, FG-3810A, FG-3810D, 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-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, FFG-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-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-3240C, FCR-3600C,FCR-5001C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.4
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D **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, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN	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

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2

Model	Firmware Version
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-200D, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.2
FortiMail: FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1.4
FortiMail: FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0.7

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-3500D	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-5902D	5.2.0

Model	Firmware Version
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-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.7
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64	5.3.3
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D **FortiCache VM:** FCH-VM64	3.0.0 and later

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.4.0.

Compatibility issues with FortiOS 5.2.7

The following table lists interoperability issues that have been identified with FortiManager version 5.4.0 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 5.4.0 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 5.4.0 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 5.4.0 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 5.4.0 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.

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

Device Manager

Bug ID	Description
307184	The cluster members of FortiGate-3200D are not displayed on FortiManager.
306284	FortiManager installs virtual-switch and system interface in a wrong order.
305187	FortiManager shows the same installed policy package name for two different VDOMs.
305044	The maximum number of VLANs per interface for FGT-30D is incorrect.
302972	FortiManager does not support FortiCarrier-3200D-DC.
300563	When users are scheduling a firmware upgrade, the date may be shown as NaN/NaN/NaN.
299947	Configuring the prefix value in router prefix list on a 64 bits platform may return “runtime error 23: beyond the boundary”.
297897	Interface associations may be lost for address objects when a VDOM has dynamic mappings overriding the originally imported global objects.
296946	Import operation identifies constant conflicts for various objects between UNSET and EMPTY values.
295908	Under the Device Manager of FortiManager, the FortiGuard License of FortiGate is shown as Unknown.
295861	Users cannot configure multiple DNS servers on the interface editing page.
295606	Invalid IP range is defined on FortiManager for a dial-up IPSec VPN.
294795	Some attributes of CLI-Only objects have default interface/access list selected and they cannot be removed.
294746	The "config log disk setting" configurations should not be modified when it is imported to a model device DB.

Bug ID	Description
294549	FortiManager may not bring up FGFM tunnel during the installation process.
294179	Users are unable to import fwpolicy-implicit-log setting to ADOM.
294162	Changing the fwpolicy-implicit-log setting at the device level does not change the Policy Package status.
293842	FortiManager is unable to import firewall policy if virtual-wan-linked interface is used in a Virtual IP object.
292218	FortiManager returns the “runtime error 89: duplicate ip in the list” error message when creating DHCP relay.
291625	FortiManager should not allow user to add "ha-mgmt-interface" as interface into "local-in-policy".
290999	Users cannot configure the DHCP Relay on Hardware Switch interface when it is set to Internal.
289515	FortiManager should not allow users to create a Static Route with a Distance Value equal to zero.
288495	Users may not be able to delete a VDOM via the Virtual Domain menu under Device Manager.
288184	When the install Wizard is canceled, the tasks stop working in the task monitor.
287885	FortiManager cannot View Detail and Download Conflict File during the policy package import process.
287381	The Device Template cannot be used if the DNS or NTP `source-ip` is set.
286227	After editing an interface filtered zone, the Dynamic Zone Mapping pop-up does not apply the changes to the filtered entries; it removes the filtered entries upon validation.
285835	All the ADOMs created by "Import Device List" are in Normal mode with VPN management "Central VPN Console".
284806	Search Group function does not work in the context of adding a device.
284080	During the policy package import process, FortiManager cannot *View Detail* or *Download Conflict File*.
282048	If a user enters a full or partial serial number of a HA slave unit, the *Search* function does not work.

Bug ID	Description
281563	When setting channel bonding to either 40MHz or 80Mhz, FortiManager is unable to save the change.
281328	HA-reserved Management interface should only appear in the ADOM with the management VDOM.
279181	FortiManager may not be able to import an IPS custom signature.
278968	FortiManager cannot add descriptions to the MAC address list under a DHCP server.
278634	FortiManager may not be able to add an extra source address in an existing policy route.
278625	Tooltip for the Status column of an administrator displays "Enabled" or "Disabled" instead of "Logged on"/"Not Logged on".
278565	The web filter profile setting *Rate images by URL* does not work.
278493	When editing a zone from the GUI, the FortiManager is unable to delete the device interface.
278485	FortiManager cannot set Phase2 `auto-negotiate` parameter.
278484	Cloning static route returns: *runtime error 33: duplicate*.
278483	FortiManager cannot select *main* or *aggressive* mode when defining a new Phase1.
278164	Interface page cannot load because of the missing VDOM setting in the `mgmt` interface.
277778	Deleting an SSID from the WiFi Template may not update the device database.
276174	When editing a VLAN or interface, there is a typo "Map to Policy Interface".
274490	When the user cancels editing an interface, the FortiManager may direct to a different interface list.
273905	When editing a system interface, FortiManager returns *fail:[objectObject]* error message.
271807	FortiManager cannot recognize the SNMP Community Host Interfaces of FortiGate HA.
271286	FortiManager does not allow users to upload images larger than 6KB in a Replacement Message.
270752	When editing a zone, the FortiManager is missing the `Block intra-zone` traffic option.

Bug ID	Description
268732	FortiManager unsets the source-ip of FortiAnalyzer log settings in System Template during installation.
264679	Package status remains Modified after a restricted admin makes changes and does an installation.
262574	JSON query JSON for multiple Phase2 associated with Phase1 support.
256571	*Collapse All* action no longer works when using a Policy Package with large number of policies and/or Section Titles.
255173	When changing a SSID interface to "Local bridge with FortiAP's interface", the input for pre-shared key is missing.
230400	Device Manager column filters are not persistent.
219930293949	Add link status in the Zone and Interfaces page.

Global ADOM

Bug ID	Description
277330	Assigning a global policy package should trigger the ADOM policy packages to update their status to "Modified".
280009	FortiManager cannot import a CA certificate in Global ADOM and configure the SSL/SSH Inspection Profile when selecting that CA Certificate.
288087	After upgrading to build B0724, Global Policy changes are not pushed to the ADOM level.

Policy and Objects

Bug ID	Description
295827	When there are a large number of packages and policies, the "where used" function may stop working.
212707	The *Search* field cursor on a policy package and on a Firewall address object is not at the same place.
233189	IPSec phase 2 selector does not support IPv6.

Bug ID	Description
238233	The Create New option of the Web Proxy Forwarding Server drop down list does not work as expected.
255211	Scrolling for policies with the scroll wheel does not display all the policy entries.
256261	FortiManager will always install `profile-protocol-options` on a policy with an IPS sensor.
263459	Creating or importing a local certificate may cause issues with the SSL Inspection Profile.
263471	After editing an address object, the FortiManager may not be able to display the object name if it contains the \ character.
265261	FortiManager cannot disable *SSL/SSH Inspection* from the Explicit Proxy Policy.
268222	IPS Signatures should also be visible under Global Object IPS Sensor profiles.
268696	*Used* for a Service Object does not work on Internet Explorer 11.
275241	*Copy* does not work when IP Pool's `arp-intf` is configured within a zone.
275568	After submitting FortiClient XML configuration changes, the changes are not saved.
276470	Changing the Advanced Options settings under the Web Filter Profile may not be properly applied in the ADOM database.
276806	Scheduled installs from a TACAS+ wildcard user does not work as expected.
277061	Web URL filter entries with more than 65 characters are truncated.
277071	There is a performance issue in the *Display* and *Search* interfaces.
277711	After selecting *Edit Interface Map*, FortiManager does not list the Zone.
278089	When *Workspace* is enabled, FortiManager may fail to import the device. *Failed to commit changes to DB* error message may appear.
278357	FortiManager is unable to identify a device interface, when *per-device mapping* is enabled, to a policy interface or device zone.
278637	The FortiManager may not be able to edit an interface from the displayed Search Results.
279439	After removing members from a VIP group, the change may not be saved.
279534	FortiManager is unable to view or use imported CA certificates.

Bug ID	Description
280112	The `.` character is not allowed for a LDAP username.
280324	When configuring `ftgd-wf` categories on FortiGate 4.3 devices, *Disable* and *Enable* functionalities should be implemented.
280607	If a global policy is configured when an address that has *per-device mapping* enabled, the mapping is lost on policy import.
280875	In the SSL VPN Portal, users cannot disable the *Include Login History* option.
281241	*Copy* does not work when installing a 5.0 Policy Package to a 5.2 FortiGate device.
281511	FortiManager cannot display groups in LDAP Browsing.
283754	IPS signatures are not updated within the IPS Sensor Profiles.
283950	The Policy Search feature does not work correctly with collapsed sections.
284319	FortiManager reports the following error: *Install failed(dev-related info was changed, install it first)* during Policy Installation.
284422	Modification of the `Block intra-zone` setting is not installed in the FortiGate.
284977	When *User Bookmarks* are disabled, pre-defined bookmarks are not available.
285408	When the *Save* button is active, the *Toolbar Install Wizard* is not grayed out.
285504	Section View is not available if the name of a policy package contains the slash ("/") character.
285530	FortiManager removes the WANopt peer from the server configuration.
285586	The Preserver Client IP option of Load balance VIP is not available when HTTP(S) Multiplexing is not selected.
286119	Dynamic Mapping for a Global Address Object is not installed into the FortiGate device.
286706	The PAC file size is inconsistent between the FortiGate and FortiManager.
288091	When a Per-Device Mapping is configured on a Load Balance Object, FortiManager shows the *Loading Aborted* error on the Virtual IP page.
288226	If a FortiGate device is removed with Dynamic Mapping configured on the objects, some object pages display the *Loading Aborted* error message.
288655	The Policy interface selection drop down list does not show zones or interfaces.

Bug ID	Description
288704	WAN optimization cannot be enabled via FortiManager.
290213	Editing URL Filter type should only save the edited entry without keeping the original entry.
290252	FortiManager returns the *Runtime Error 131* when right-clicking to add a WAN-load-balance interface.
290986	FortiManager prompts a runtime error while configuring address groups with URL objects.
291043	An object change pushed by a restricted admin results in the conflict state of the policy package.
291163	Warning message is not always displayed when adding duplicate address objects.
291730	Preview prompts the "Cannot open file" error message when SSID from WiFi template has overlapping IP addresses.
292348	Changing the action on any FortiGuard category within the webfilter profile under a 5.0 ADOM should not set category override and unset all exempted categories.
293431	A canceled Policy Package Installation preview makes changes to Device DB when Workspace is enabled.
293594	Users cannot use special characters in PKI user’s Subject field.
293941	Making changes in the SSL-VPN portal may not trigger changes in policy package status.
293949	FortiManager cannot manage all SIP settings in a VOIP profile.
295084	A new UUID is created for a dynamically mapped address with a different comment for every import.
295537	Dynamic mapped objects show "N out of 0" for a FortiCarrier ADOM.
295540	FortiManager should not install "report layout - purge" with every policy package installation.
295557	Changes to User Group that reference an IPSec Phase1 object are not installed.
295745	When installing a v5.0 policy package to a v5.2 FortiGate device, firewall rules are not installed in the correct order.
295828	Multiple users cannot generate preview at the same time.
295944	Installation of a policy package changes the UUID of identity policies.

Bug ID	Description
296766	Installation will fail when an interface of a policy is changed to the management interface.
299515	FortiManager does not report an error when users choose an SSL-VPN interface to be a member of zone.
300814	When there are a large number of firewall policies, it may take a long time to clone/edit a policy.
300986	Local interface names that contain space can lead to dynamic mapping config problems.
301247	Setting a Virtual IP as destination in a policy does not work when the External Interface binding of the Virtual IP is different from the destination interface in the policy.
301695	Field Service and Schedule are ignored during policy consistency check.
302870	Policies inside a renamed policy package will have an empty drop-down list for Source Interface and Destination Interface.
302913	Changes of the order of objects under identity-based-policy will not be installed on FortiGate.
305726	FortiManager cannot install guest user group *authtimeout* to FortiGate.
306434	The “Where used” function may show dynamic mapping of an address that has already been deleted.

Revision History

Bug ID	Description
268732	When installing, the FortiManager tries to unset the source IP of a FortiAnalyzer device.
270711	When a FortiGate is added to a FortiManager, the formatting is not correct causing usability issues when trying to *diff* revisions.
277294	FortiManager removes multicast objects and policies unexpectedly.
279075	After upgrading, FortiManager sets up `tcp-portrange = 0` for some FortiOS versions.
280187	FortiManager is unable to retrieve 4.3 ADOM configuration. *Failed to reload configuration. Max entry.object wireless-controller error* message appears.

Bug ID	Description
280193	When FortiGate HA is enabled, FortiManager disconnects mac addresses for VDOM-link interfaces.
281050	FortiManager sets *802.11n,g-only* band option as *802.11n g-only* to the wtp profile.
282097	FortiManager does not install security-groups to Captive Portal.
283961	Changing firewall address type from FQDN to IP results in installation failure.
286392	FortiManager rests the IPS block duration if *Quarantine* is disabled.
286415	FortiManager removes or inserts *None* objects when installing 5.0 ADOM policies to FortiGates running FortiOS 5.2.
286686	FortiManager should use set auth radius when the security mode requires RADIUS.
286872	After upgrading the ADOM from 5.0 to 5.2, FortiManager modifies the Global Firewall Policy UUID.
287879	Policy Package installation failure occurs following FortiManager upgrade from 5.2.2 to 5.2.3.
287881	Incorrect Revision History entry is highlighted.
287882	Nested dynamic address group changes are not installed.
291044	No auto ADOM revision is generated for restricted admin users during partial-installation.
292459	SSID configured with "captive portal" as the security mode and "Disclaimer Only" as the portal type does not get pushed to the FortiGate device.
295338	ADOM revision may not able to revert to a previous version after any type of changes.
307894	FortiManager may fail to create a VDOM on FortiGate-60D.

Script

Bug ID	Description
300409	Script for Radius server configuration leaves secondary-secret unencrypted in the execution history log of Task Monitor.
259444	Deselecting the "Advanced Device Filter" option for a script should clear the device filter.

Bug ID	Description
286111	TCL Script stops working if the FortiGate SSH Port Number is not 22.
290585	FortiManager should allow importing scripts via SCP.
301394	No error is returned when function createScript misses parameter "target".

Services

Bug ID	Description
277389	FortiManager stops working when `serviceaccess fclupdates` is enabled on a port number that is not 80.
279272	FortiGuard shows the Pending status for databases that FortiGate is not subscribed to.
279475	Using an image downloaded from FortiGuard, FortiManager is not able to upgrade a FortiGate's device firmware.
287811	The um_db_service process may consume high IO resource.
294076	When there are many requests, FortiManager VM users may not be able to log in.
294410	Null entry for server-access-priorities causes system to freeze on reboot and return the "cli 162 die in an exception in line -1: (null)" error message.
298651	When receiving auto-updates from a large number of FortiGates, FortiManager may run out of memory.

System Settings

Bug ID	Description
227133	The setup of a FortiManager HA cluster should not be allowed when the master and slave units have mismatched licenses.
240128	FortiManager does not encrypt schedule backup with a password containing 17 characters.
242337	The SNMP trap message is not proper when the administrative status of an interface is changed.

Bug ID	Description
247941	When logging in Wildcard users with a read-only profile on the HA slave unit, the Dashboard is blank
277293	When changing the HA Settings, it may cause the unrelated HA members to become out-of-sync and may trigger an offline cluster.
279186	When there is an on-going retrieve or installation task, the backup file may become corrupted.
279415	Authentication should not time out after a few seconds with two-factor authentication.
280717	Task Monitor entry refers to `rootp` ADOM instead of `Global` for Global Policy Assignments.
281348	FortiManager removes all policy packages and objects after upgrading ADOM.
285956	A device level install is incorrectly logged as an Install Package in the Task Monitor.
286889	When the Global Database is upgraded from 5.0 to 5.2, it returns the error: `fail (errno=-1):unknown`.
289207	After a configuration change on FortiGate, FortiManager may falsely report that certificate private keys have changed.
291025	Remote administrators are unable to approve a session under Workflow mode.
296028	When RADIUS authentication is configured with wildcard authentication, some actions are not logged with the correct user name.
296235	Multiple incorrect webfilter_ftgd_local_rating messages are reported in the Event log during the import operation.
299728	"Admin-lockout-threshold" and "admin-lockout-duration" do not work for SSH access.
303922	Users cannot select individual TLS versions.

VPN Console

Bug ID	Description
269222	FortiManager is unable to remove VPN Console > External Gateway > Hub IP value once configured.
271687	After upgrading, FortiManager prompts the VPN Console to regenerate the pre-shared key.

Bug ID	Description
272932	After modifying a user group, the dial up spoke user is not updated.
289900	The VPN Console should not generate a Status Route on the hub for its own protected subnet.
301375	Adding or deleting a Spoke in a Star topology VPN will change the policy package status of existing Spokes.

Others

Bug ID	Description
280054	"Diagnose dvm check-integrity" reports "Checking duplicate device vdoms" errors without fixing them automatically.
227634	FortiManager should allow backup via SCP.
253961	Display the system uptime in a readable format instead of the Linux Epoch format.
267042	WSDL file should be generated with the right version number for ADOM 5.2.
274415	SNMP trap OID is not in the MIB.
277392	The FortiManager may take longer than expected to upgrade.
279370	After upgrading, FortiManager cannot display policies if the policy package does not have a name.
279900	FortiManager does not display Install On targets in CLI Command output: `execute fmpolicy print-adom-package<ADOM_ID><POLICY_PACKAGE_ID><Cat-egory>all`.
280993	FortiManager does not print out all the debug messages in the console.
281172	When the `exe fmpolicy check-upgrade-object` command is run, FortiManager may stop working.
281263	The legacy XML API `<getInstLog>` does not work in *Workspace* mode.
281319	FortiManager may not currently support: FG-3810D, FG-3810D-DC, FG-3700DX, FG-3200D, FG-70D-POE, FGV-40D2, and FGV-70D4.
282094	FortiManager does not support `HTTP "Expect: 100-continue` mechanism for JSON request.

Bug ID	Description
282187	Certificate setting cannot be changed on the FortiManager slave unit.
284528	Users are unable to use JSON API to get the ADOM Policy Package Exclusion List for a particular Global Policy Package/ADOM combination.
284677	Policy Package Status is changed to Modified after upgrade.
288160	FortiManager cannot install a policy via the `installConfig` SOAP XML request; it returns the *no write permission* error message.
292138	RADIUS wildcard user cannot login with JSON API.
294191	Users may not be able to install policy via JSON APIs with workspace enabled.
294879	Within a HA cluster, the password for the admin account is not synchronized to slave when password policy is enabled and triggered.
295629	Users cannot filter “pm/config/adom/<adom>/_package/status” with JSON APIs.
295715	FortiManager does not have a CLI command to retrieve sensor detail or sensor list.
296788	Users cannot use the Provisioning Template name string as a parameter in the CLI command “execute fmpolicy print-prov-templates”.
297164	Users are not able to move and rename a Policy Package at the same time.
298716	In XML APIs, the execSecurityconsoleInstallPackage call with flag “preview” returns error message “runtime error -1: invalid value”.
299507	The result formats of different JSON requests should be consistent.
301181	JSON API call "pm/config/adom/<adom>/_rule/list" does not return the same information as the output from FortiOS CLI command "get ips rule status".
302389	The CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, and CVE-2015-3196 vulnerabilities have been addressed.
303117	After removed the secondary FortiManager from a FortiManager cluster, FortiGate does not remove the serial number of the secondary FortiManager from its configuration.
306958	The CVE-2016-0777 and CVE-2016-0778 vulnerabilities have been addressed.
307237	Users with two-factor authentication cannot log on via JSON APIs.
307453	Multiple JSON commands can be executed without authentication.
307847	Removed the maintainer account from FortiManager.

Known Issues

The following issues have been identified in 5.4.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
307995	Users cannot save alert email settings at device level.

Policy and Objects

Bug ID	Description
308211	Policy package status may be changed to "modified" after importing another policy package.
295333	FortiManager should be able to disable logging within an IPS Sensor.

VPN Manager

Bug ID	Description
307433	FortiManager converts a /32 subnet into an IP address when configuring IPSec phase 2 settings.

Others

Bug ID	Description
310570	FortiSwitch device information is missing on dashboard.

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	✓		✓	
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