FortiManager - Release Notes

VERSION 5.6.0

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

April 23, 2018

FortiManager - Release Notes

02-560-442453-20180423

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-07-27	Initial release of 5.6.0.
2017-07-28	Added 443050 to *Known Issues* > *Device Manager*.
2017-07-31	Added a note to the *Upgrade Information* > *Upgrading to FortiManager 5.6.0*.
2017-08-03	Added bugs to Known Issues.
2017-08-09	Added 444270 to *Known Issues* > *FortiGuard*.
2017-08-14	Added *Special Notices* > *Port 8443* reserved.
2017-08-15	Added *Product Integration & Support* > *FortiClient* > *5.4.0 and later, and 5.6.0* support.
2017-08-16	Added additional information to *Upgrade Information* > *One-click ADOM upgrade to FOS 5.6 is not supported in FortiManager 5.6.0* note.
2017-08-21	Updated Special Notices. Added 380790 to *Known Issues* > *Others*.
2017-09-01	Updated *Product Integration & Support* > *Web Browsers*. Added 416840 to *Known Issues* > *Others*. Removed *Management Features* support from *Product Integration & Support* > *Feature Support* > *FortiSandbox*. Added *Reports* support to *Product Integration & Support* > *Feature Support* > *FortiSandbox*.
2017-09-13	Removed Compatibility issues with FortiOS 5.0.4 and 5.0.5 as FortiManager 5.6.0 does not support FortiOS 5.0.X.
2017-10-11	Updated *Product Integration & Support* > *Feature Support* > *FortiAnalyzer* > *added Reports and Logging*.
2017-10-23	Added 369270 to *Known Issues* > *Logging*.
2017-10-27	Added note about LENC device support and added 395060 to *Known Issues* > *Device Manager*.
2017-10-31	Added 423155 to *Resolved Issues* > *Device Manager*.
2017-11-20	Added 2.4.0 and 2.4.1 support to *Product Integration & Support* > *FortiSandbox*.

Date	Change Description
2017-11-28	Added a note to *What's New* > *Security Fabric Management* > *Managed FortiAnalyzer*.
2017-11-30	Added a note to *Upgrade Information*. When upgrading from 5.2, an Import Policy Package should be preformed on all FortiGates using Local-In-Polices.
2018-02-21	Added information about upgrading from 5.2.x.
2018-04-23	Added *Color themes* to *Special Notices*.

Introduction

This document provides the following information for FortiManager 5.6.0 build 1557:

- Supported models
- What's new in FortiManager 5.6.0
- 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 5.6.0 supports the following models:

FortiManager	FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, 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).

Minimum screen resolution

The recommended minimum screen resolution is 1280 x 800. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

What's new in FortiManager 5.6.0

The following is a list of new features and enhancements in 5.6.0. For details, see the *FortiManager Administrator Guide*:

Fortinet Security Fabric Management

Managed FortiGate Security Fabric cluster

- Manage FortiGates in a Security Fabric cluster as if they are a single device
- View the topology of the FortiGate Security Fabric cluster from the Device Manager

FortiSwitch Manager

A new FortiSwitch Manager module that supports provisioning templates, central deployments and status monitoring for managed switches.

Managed FortiAnalyzer

- Support managed FortiAnalyzer by adding a FortiAnalyzer unit to an ADOM in FortiManager.
- Automatically synchronize the device configuration on FortiManager to the managed FortiAnalyzer.
- View log analytics, monitor events, and generate reports from the single FortiManager console.
- Modify a policy via a policy ID from Log View and view policy related logs from Policy Package.

Managing FortiAnalyzer is not available when ADOMs are enabled and in Advanced mode.

Policy Packages

Central DNAT

Central DNAT is now available on a per policy package level. You can add a central DNAT entry by creating a new Virtual IP or by using an existing Virtual IP. These DNAT entries are shared amongst all the policy packages.

Traffic shaping policy package for ADOMs

- Support Global traffic shaping policy
- Allow both header and footer traffic shaping policies just like the regular header and footer policies
- Support for traffic shaping policy packages at the ADOM level.

VPN Manager

Set priority on VPN Gateway interface

You can set priority on VPN Gateway Interface from the FortiManager GUI by using the Advanced Options section. The priority information is now saved in the generated VPN routes.

VPN Gateways on Google map

Display VPN gateways on Google map and monitor the VPN tunnel traffic in real-time

FortiAP Manager performance improvements

Improved the FortiAP Manager's performance for managing deployments with more than 10,000 FortiAPs.

FortiGuard Package management usability

You can view the service status by managed device or by FortiGuard security content package.

FMG-VM minimum configuration check

For FMG-VM running in VMware hypervisor, the GUI displays a warning if the VM installation does not meet the minimum required 2x vCPU and 4GB memory.

Add-on license for high-end appliances

- Allows additional devices/vdom on high-end appliances; additional devices are added in batches of 100
- Up to 100,000 devices/vdoms maximum on FMG-3900E
- Up to 8,000 devices/vdoms maximum on FMG-3000F

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.6.0.

Color themes

You can choose a color theme for FortiManager GUI. Each release of FortiManager includes the same number of color themes; however, some of the color themes change each release. This section lists the names of the color themes in the CLI and the GUI.

After you upgrade to FortiManager 5.6.0, the color theme for FortiManager GUI resets to the default color theme if your selected color theme has been removed from FortiManager 5.6.0.

Following is a list of color themes that were removed from FortiManager 5.6.0:

- `city`: City
- `galaxy`: Galaxy
- `landscape`: Landscape
- `purple-ink`: Purple Ink
- `skyline`: Skyline
- `snow`: Snow
- `succulents`: Succulents
- `sunset`: Sunset
- `tree-ring`: Tree Ring

Following is a list of new color themes for FortiManager 5.6.0:

- `astronomy`: Astronomy
- `binary-tunnel`: Binary Tunnel
- `fish`: Fish
- `linked-world`: Linked World
- `panda`: Panda
- `parrot`: Parrot
- `penguin`: Penguin
- `polar-bear`: Polar Bear
- `technology`: Technology
- `twilight`: Twilight

Following is a list of color themes that remained the same for FortiManager 5.6.0:

- `aquarium`: Aquarium
- `autumn`: Autumn
- `blue`: Blueberry
- `diving`: Diving
- `dreamy`: Dreamy

- `green`: Kiwi
- `honey-bee`: Honey Bee
- `melongene`: Plum
- `mountain`: Mountain
- `northern-light`: Northern Light
- `red`: Cherry
- `spring`: Spring
- `structure-3d`: 3D Structure
- `summer`: Summer
- `winter`: Winter

FortiGate VM 16/32/UL license support

FortiOS 5.4.4 introduces new VM license types to support additional vCPUs. FortiManager 5.6.0 supports these new licenses with the prefixes of FGVM16, FGVM32, and FGVMUL.

Hyper-V FortiManager-VM running on an AMD CPU

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

IPsec connection to FortiOS for logging

FortiManager 5.4.2 and later does not support an IPsec connection with FortiOS 5.0/5.2. 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.

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 or later before applying the new license to avoid benign GUI issues.

System Configuration or VM License is Lost after Upgrade

When upgrading FortiManager from 5.4.0 or 5.4.1 to 5.4.x or 5.6.0, it is imperative to reboot the unit before installing the 5.4.x or 5.6.0 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 and later no longer supports FortiOS 5.4.0. Please upgrade FortiGate to 5.4.2 or later.

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

Local in-policy after upgrade

After upgrading to FortiManager 5.4.1 or later, 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 and later 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 tlsv1
end
```

Port 8443 reserved

Port 8443 is reserved for `https-logging` from FortiClient EMS for Chromebooks.

Upgrade Information

Upgrading to FortiManager 5.6.0

You can upgrade FortiManager 5.4.0 or later directly to 5.6.0. If you are upgrading from versions earlier than 5.4.x, you should upgrade to the latest patch version of FortiManager 5.4 first.

When upgrading from FMG 5.2, an *Import Policy Package* should be performed on all FortiGates using *Local-In-Polices*. As of FMG 5.4, these are handled in Policies & Objects.

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.

One-click ADOM upgrade to FOS 5.6 is not supported in FortiManager 5.6.0.

You will need to create a new 5.6 ADOM and move your 5.6 FortiGates (or add new 5.6 FortiGates) to this 5.6 ADOM. Then, you use the *Import Policy* function to create the ADOM `db config`.

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 5.6.0 support

The following table lists 5.6.0 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects. • Mozilla Firefox version 54 • Google Chrome version 58 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier	• 5.6.0 • 5.4.1 to 5.4.5 • 5.2.8 to 5.2.10 FortiManager 5.6.0 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 28. • 5.2.7 FortiManager 5.6.0 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 28. • 5.2.6 FortiManager 5.6.0 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 28. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.6.0 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 29. • 5.2.0 FortiManager 5.6.0 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 29.
FortiAnalyzer	• 5.6.0 • 5.4.0 to 5.4.2 • 5.2.0 to 5.2.10 • 5.0.0 to 5.0.13
FortiCache	• 4.1.2 • 4.0.0 to 4.0.4
FortiClient	• 5.6.0 • 5.4.0 and later • 5.2.0 and later

FortiMail	• 5.3.7 • 5.2.9 • 5.1.6 • 5.0.10
FortiSandbox	• 2.4.1 • 2.4.0 • 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 19.

Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS
	• Citrix XenServer 6.2
	• Linux KVM Redhat 6.5
	• Microsoft Azure
	• Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2
	• OpenSource XenServer 4.2.5
	• VMware
	  • ESX versions 4.0 and 4.1
	  • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5

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

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

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

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓

Language	GUI	Reports
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 5.6.0.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E,3G4G-INTL, FG-30E,3G4G,NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG81E-POE, FG90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-240D, FG-240-POE, FG-280D-POE, FG-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, FG3240C, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D **FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E **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, FG-3815D-DC **FortiGate Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.6

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

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

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-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6

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 5.6.0.

Compatibility issues with FortiOS 5.2.10

The following table lists interoperability issues that have been identified with FortiManager version 5.6.0 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 5.6.0 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 5.6.0 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 5.6.0 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 5.6.0 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.

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.

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.

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

AP Manager

Bug ID	Description
286686	When WiFi template specifies a security mode requiring RADIUS, FortiManager may incorrectly set `auth usergroup` in the VAP definition.
400116	Users may not be able to manage Local WiFi from FortiManager.
400116	Users may not be able to assign wtp profile for Local-WiFi.
401921	The number of allowed FortiAPs may be different between FortiManager and FortiWifi-30D.
407822	Users may not be able to configure *User Groups* and the Exempt List for SSID profiles.
434610	Channel Width may be saved as 20MHz for 802.11ac/n radio and 802.11ac radio in AP profile.

Device Manager

Bug ID	Description
249922	Device list may not record HA information for devices.
305734	The folder list in import wizard may not be in alphabetical order.
372581	`dns-service` may be set to local if users set *Use system DNS setting* from GUI.
390931	If a `phase1-interface` is monitored by another, it may need to purge twice to remove this interface.
391674	FortiManager may not support changes with `snmp-index`.
393629	When users clone a static route, the device entry may not be displayed on GUI.
393641	Policy package status of a device may become modified after a user added another device and imported policy from it.

Bug ID	Description
394294	The `same` routing table may be displayed for different VDOMs.
397520	After FortiManager upgrades to 5.2.9, it may incorrectly install np6 session-collector-interval 8 to 5.2.4 FortiGate.
399646	SLBC may intermittently lose connectivity to FortiManager.
400091	The installation order may be incorrect for policies with `virtual-wan-link` interface.
400245	FSSO configuration at device level may not be able to display FSSO groups.
401369	A VAP interface that used by a switch interface may cause a copy fail.
401844	FortiAnalyzer settings may be missing in `CLI-Only` object.
402005	Some E series FortiGates may nave incorrect config `logdisk=0`.
404083	If two static routes share the same gateway, the one without `internet-service` may get deleted during installation.
404470	Users may fail to upgrade low-end FortiGates from FortiManager.
404708	Installations may fail due to outdated FAP200A default wireless profile.
405227	Installation may hang if an interface has *Default Mapping* enabled with the value being *NULL*.
407982	There is no option to enable SNMP Agent for FortiGate in device system template from GUI.
408927	Static routes with named address on the same interface may get deleted upon installation to FortiGate.
411195	Users may fail to import a revision.
412145	Users may not be able to add NTP server by DNS name in provisioning template.
412158	FortiManager may accept `any` for `Interface-passive`.
416792	FortiManager may display the FortiGate HA status as up when it is in standalone mode.
417195	FortiManager may be slow to respond when there are many FortiExtenders attached to the managed FortiGates.
421055	`local-gw` setting in VPN IPsec Phase 1 may not be saved from GUI.
421866	`block intra-zone traffic` setting may be lost after users remove an interface from an ADOM interface mapping.

Bug ID	Description
423155	GUI server side change from simple http request to web-socket.
434285	The replaced device may not go into unregistered list.
437583	*Connect to CLI via* may always connect to a same device if there are multiple FortiGates behind NAT.

Global ADOM

Bug ID	Description
421773	Global policy package assignment may get stuck at 70%.
421979	Assigning a global policy package may not work as expected.
435322	Web filter override change in Global ADOM may not trigger the *assign* feature for policy packages.
438641	Adding an ADOM to Policy Package assignment page may cause the other ADOMs status to be changed to *Pending changes*.
438643	Users may fail to clone a policy package in Global ADOM if its name starts with “Global”.
439743	Excluding one Policy Package in Global ADOM assignment page may cause Policy Package status in other ADOMs to be modified.
440107	Global ADOM may fail to be upgraded if there are invalid dynamic mappings.

Policy and Objects

Bug ID	Description
262010	Users may not be able to filter policies according to their status.
274882	Subnet mask with notation of /x style may cause installation to fail.
281820	FortiManager may not support *central-snat-map* creation from GUI.
357218	Users may not be able to reorder Static URL filter in Web Filter profile.
366996	Sometimes install preview may show incorrect content when users are installing several policy packages.

Bug ID	Description
370112	Users may not be able to create or edit SSL/SSH profiles.
376516	Users cannot choose *Suspicious Files Only* for AntiVirus Profile in FortiManager from GUI.
379128	In SSL/SSH Inspection profile, the drop down list of CA Certificate may be empty.
379191	Users may not be able to select a URL address as the destination address from the *Explicit Proxy Policy* in the GUI.
383572	*Unrated* may be available as a category for SSL Inspection Exemption.
389515	Users may not be able to edit or delete a service category with `&` in its name.
389715	GUI may not accept multiple ports in ssl-ssh-profile.
394088	FSSO settings may get purged during installation.
396422	Users may not be able to search for *Address Objects* with CIDR notation in the Policy View.
400247	FortiManager may not automatically *set rsso enable* when creating RSSO objects from GUI.
400354	Deleting a global policy package assignment may not remove the global policies assigned to the ADOM.
400615	Locking a policy package by clicking on its name may incorrectly lock another package.
400844	If associated interface of a dynamic firewall address is different from that on device database, it may trigger a copy failure.
401079	Users may not be able to create a VIP with *Dynamic Mappings* if *Configure Default Value* is off.
401366	FortiManager may show incorrect Security Profile details.
401475	Viewing VIP objects may be slow if there is a large number of a VIP mapping.
401476	Viewing IP pool objects may be slow.
401481	Changes for web categories and addresses under SSL exemption in SSL/SSH profiles may not be saved in GUI.
401485	Policy installation to nested groups may not work.
401487	Sometimes GUI shows “Nothing to install” while the installation task is running

Bug ID	Description
402112	FortiManager may not automatically add `attack_id` for custom IPS signatures if they do not have one already.
402261	Duplicate Dynamic Mappings are created if some VIP objects in a VIP group reference a Zone Interface.
402685	Copy error may occur if users are using a local certificate with global range from a VDOM.
404895	Install policy package may fail if a dynamic VIP is bonded to an interface which also has dynamic mappings.
404971	The GUI may show an empty dynamic mapping list after users edit the mappings.
405425	Policy Package installation to FortiGates may fail if it includes a VIP that has been renamed recently.
405430	Installation may hang if there is a large number of AD groups.
406105	FortiManager may allow user to use un-supported filter in *Application Control for Filter Overrides*.
406781	Search may not work in LDAP user objects.
408027	There might be security console crashes if some address groups have empty members.
408436	The action *Reset* may not be displayed for *Application Control* in FortiManager GUI.
409025	Reordering static urlfilter may not work.
410727	Invalid global policies may be copied to ADOMs during assignment and cannot be deleted.
410776	A cloned object may not have the same group membership as the original one.
411337	Action *Proxy* is missing for *tcp_syn_flood* under DoS policies in GUI.
411650	The URL table ID may also be cloned when a web filter profile is cloned.
412591	*Where Used* may not work for 5.0 ADOMs.
412848	Policy table view may only accept 35 characters at the maximum for comments.
415296	Comments for IP Pools may not be shown in the list page.
416099	Tags may not be displayed.
416315	`fwpolicy-implicit-log` may be unset after a global policy package has been assigned to an ADOM policy package.

Bug ID	Description
416530	Some object groups may not be able to be added to an installation target of a specific policy.
416813	*Policy Import* may fail due to the failure to create mappings for VPN SSL web portal.
422780	VIP Groups with dynamic mappings may not install.
423757	A wildcard URL entry with action block may be moved to the first in the URL Filter list in Web Filter profile.
433623	The policy interface pair view may not pair properly, duplication may occur.
433866	Installation may be blocked if a zone name is the same as a member interface name.
434671	When users try to add a new device to *Installation Target* via Search function in GUI, it may remove all existing installation targets.
435211	IPS custom signatures with `--crc32` may not be created on FortiManager.
435320	Search may not work for imported dynamic address objects that are imported within a dynamic address group.
435971	URL filter rules may be re-ordered following FortiManager upgrade.
436676	Users may not be able to create or copy and paste Explicit proxy policies.
436883	Updating a policy may take a long time if there are many policies.
437238	Sometimes Web Filter may display web elements.
438584	Import policies may get stuck if there is a firewall address with empty address type.
439047	Policy hit count may be also copied if users copy and paste a policy.
439487	After users paste a policy below another one, the page may automatically scroll to the top.
439749	Deleting a dynamic mapping of an object may cause status of other Policy Packages referencing this object to be *Modified*.
440266	Users may not be able to delete Source Address “all” from explicit proxy policies.

Revision History

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

Script

Bug ID	Description
386276	Users may not be able to configure *Recurring time for Schedule* enabled scripts from the GUI.
389897	Running a script may fail if it tries to set a one-time schedule with the month being 1 digit.
401474	Running scripts on Nested Groups may fail.
401486	Running a TCL script may be reported as successful from GUI while the device password is incorrect.
404065	TCL scripts with "clock" may not work.
406655	Scheduled CLI script run on remote device may be run on device db.
407797	Users may not be able to set a weekly schedule in per device script history page.
411964	In the *Device Selection* page, if you search for a new key word, the previous selection may be lost.
411975	Running a script against a group may fail.
435105	When `allow-subnet-overlap` is enabled, users may not be able to set up overlapping IP address and subnet on interface and IPSec tunnel interface by running CLI script.

Services

Bug ID	Description
411205	The command `execute fmupdate ftp import custom-url` may skip some invalid URLs in the file.
404787	Users may not be able to view and configure web proxy under FortiGuard Web Filter and Email Filter Settings.
400982	Too many FortiClients update request may cause the UDM to stop working.
418535	`fds_svrd` may take up to 100% CPU.
437194	Sometimes FortiManager may still connect directly to the servers from the FDS list although there are FDS proxy settings configured.

System Settings

Bug ID	Description
364775	The Log Receive Monitor widget may show Device ID instead of Device Name.
381189	There may not be event log generated for admin password change.
396417	Mail server connection test from GUI may fail.
401983	FortiManager may not support Radius server when secret is defined with more than sixteen characters.
402385	FortiManager may not support password with more than 32 characters for SNMP.
407916	The *Save* button may not be triggered when policy section title is changed under workspace mode.
411262	Admin user may not be able to create a session when its device manager privilege is *Read Only*.
417616	Daylight saving time for Moscow timezone may not work properly.
438586	The landing page for Restricted Admin may be different each time he logs in.

VPN Manager

Bug ID	Description
356454	SSL VPN monitor may show information for VDOMs managed by other ADOMs.
400869	If users use the Pre-shared Key option, Generate(random), for a full mesh VPN, there may be a copy fail.
401424	CPN central management ADOM may fail to upgrade from v5.2 to v5.4 due to invalid dynamic mappings.
404909	Zones and disa-up tunnels may be removed after upgrade.
405240	Users may not be able to create multiple IPSec VPN Phase 1 on a same interface.
407997	SSLVPN Monitor may not work.
408165	After removing a gateway from the VPN console, if the users try to add it back, there will be a duplicate gateway error during installation.

Bug ID	Description
413684	Creating an IPSec VPN Phase 1 with option to *Create FortiClient VPN* may fail.
417007	Changing `remote-gw` may delete and re-configure FortiGate VPNs.
417580	Deleting a gateway from the VPN topology may not remove IPsec Phase 1 and its related tunnels.
422730	Installation may fail if an address group is used in the protected subnet in the VPN.
437750	The error message is not clear when users try to add more than 10 portals.
441512	Users may not be able to use nested address groups as protected subnets.
441646	Users may not be able to install the configurations to Spoke if they only make changes on the Hub.

Workplace and Workflow

Bug ID	Description
418195	When workspace mode is enabled, GUI may hang after users switch from Global ADOM to other ADOMs.

Others

Bug ID	Description
376022	The alert *HA cluster is down* may be displayed even if the cluster is back up again.
397863	The `execute fmscript list` command may return the incorrect ADOM for a script.
399138	VM Meter service information may not be returned with JSON APIs.
401014	Apache being down intermittently may block access to GUI through HTTP or HTTPS.
401251	ADOM upgrade may fail because of `wtp-profile`.
405409	XML request `addPmConfig54AdomObjFirewallServiceCustom` may not accept the dash inside port ranges.
407889	The command `execute dmserver showconfig` may display JSON request and response before the configuration.

Bug ID	Description
409731	SNMP trap may not be sent when the interface is up.
411197	`execute fgfm reclaim-dev-tunnel` may not work for a device with existing tunnel.
413568	SNMP query for `ifInOctets/ifOutOctets` may return `counter64` instead of `counter32`.
422425	Upgrading ADOM from v5.2 to v5.4 may fail because of `tcp-portrange` syntax problems.
422627	Sometimes scheduled backups may to sftp server may fail.

Common Vulnerabilities and Exposures

Bug ID	Description
389255	FortiManager 5.6.0 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 5.6.0 is no longer vulnerable to the following CVE-References: • 2016-6309 • 2016-7052 Visit https://fortiguard.com/psirt for more information.
390355	FortiManager 5.6.0 is no longer vulnerable to the following CVE-Reference: • 2016-6153 Visit https://fortiguard.com/psirt for more information.
399178	Security hardening: admin with Read-only/None access should not get any other admin hashed password.

Bug ID	Description
404282	FortiManager 5.6.0 is no longer vulnerable to the following TMP-Reference: • 2017-0006 Visit https://fortiguard.com/psirt for more information.
405125	FortiManager 5.6.0 is no longer vulnerable to the following CVE-References: • 2017-3731 • 2017-3730 • 2017-3732 • 2016-7055 Visit https://fortiguard.com/psirt for more information.
405226	Policy Package name may be vulnaerable to XSS attacks.
408241	FortiManager 5.6.0 is no longer vulnerable to the following CVE-References: • 2016-9317 • 2016-6912 • 2016-10166 • 2016-10167 • 2016-10168 Visit https://fortiguard.com/psirt for more information.
416917	FortiManager 5.6.0 is no longer vulnerable to the following CVE-References: • 2016-10229 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.6.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
395156	If an SSID is imported from FortiGate, changes made in the SSID may not trigger installation.
397342	Users may not be able to change encrypt or disable WiFi broadcast in SSID templates via GUI.
439365	The attribute *Schedule* may be missing in AP Manager SSID configuration.
439970	*Device Category* may be shown in Compliance column without being set.
440650	Users may not be able to configure 2 DNS servers in SSID profile.

Device Manager

Bug ID	Description
395060	FortiManager may fail to add a v5.6.0 FortiGate LENC devices.
395060	Discovery of LENC devices failed.
402127	Users may not be able to create a new static route with named address in Device Manager.
434101	Users may not be able to configure Authentication Success Page in Replacement Message.
437820	FortiManager may purge SNMP and DNS settings on AWS FortiGates.
438217	FortiManager may not send Mobile FortiToken activation request.
438450	FortiExtender query may not be updated in real time.
439546	Users may not be able to de-authorize users from FortiManager.
440860	Users may fail to generate certificate with FortiAuthenticator 5.0.0.

Bug ID	Description
441237	Users may fail to create a DHCP relay server with VLAN interface from GUI.
441649	Users may fail to enable SNMPv3 in provisioning template for 5.2 ADOMs.
441754	The device revision diff may show password in plain text.
441820	FortiManager may try to unset `tcp-mss` value in device interface unexpectedly during installation.
441878	`Authtype` option both may not be supported on FortiManager under `lte-modem` settings
442327	FortiManager GUI may show minutes in unit instead of seconds for `webfilter-cache-ttl` and `antispam-cache-ttl` in *System->FortiGuard* in Device Manager.
442532	It may be slow to connect to FortiGate CLI from Device Manager Dashboard.
443050	A logging only device may not be moved to other ADOMs when FortiAnalyzer feature is enabled.

FortiGuard

Bug ID	Description
444270	FortiGuard Package Update Service Status page, may contain an incorrect Simplified Chinese translation.

Logging

Bug ID	Description
369270	FMG Slave may stop receiving FGT logs after changing device name **Workaround:** `restart oftpd on FMG slave` using command `dia test application oftpd 99`, after that oftp connections can be established and FMG slave can receive logs again from the FGT.

Policy & Objects

Bug ID	Description
403564	Users may not be able to do a partial install for an unused object.

Bug ID	Description
435779	GTP profile may not be displayed on GUI if *Security Profiles* is not enabled.
437443	Changes with Remote User Group distinguished name may not get installed to FortiGate.
438170	When users create customer service and set an iprange, `set fqdn` may be used instead of set `iprange`.
438745	Certificate selection may not get saved in Virtual Server per device mapping.
439356	Not all groups may be displayed when users try to assign a user device to a group.
439512	FortiManager may try to delete Radius user group during installation.
439594	Users may be unable to delete FSSO dynamic mappings when there are 69000 of them.
440228	Policy packages may not be listed in alphabetical order.
442104	Users may be able to configure address with unsupported type *Wildcard FQDN* for 5.2 ADOMs.
442307	In policy list page, search results may not include address groups containing the address being searched.
442769	Installation preview may get stuck at 15% following the FortiManager upgrade.

Script

Bug ID	Description
442120	On FortiManager 3000C, Running script on Remote FortiGate Directly may cause `dmserver` crash.

Services

Bug ID	Description
401746	FortiGate may not get correct webfilter license if it has FortiManager slave is configured as the override URL rating server.
437966	Downstream FortiManager may not be able to get AV&IPS signatures from upstream FortiManager.
440718	If an FOSVM joins a HA cluster as a slave when it is in unregistered device list, it may not be able to get the UTM contract from FortiManager.

System Settings

Bug ID	Description
424389	The fingerprints of certificates may not be displayed.
438424	Admin user may not be able to approve sessions in workflow mode.
439377	Duplicate event log entries may be generated for changes made on FortiManager HA master.

VPN

Bug ID	Description
442368	Users may not be able to create new or edit SSL VPN Portal profiles when workspace mode is set to workflow.

Others

Bug ID	Description
380790	Linefeed code in PAC File for ExplictProxy my change from *CR LF* to *LF*.
416840	Microsoft Internet Explorer or Edge may not completely render a page with a large set of policies or objects. **Workaround:** Please use Mozilla Firefox or Google Chrome to view the page.
442534	Out-of-Sync pop up window may not be displayed.
442695	Slave FortiGate may be wrongly counted as one device for licensing purpose.

FortiGuard Distribution Servers (FDS)

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

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

FortiGuard Center update support

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

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

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later	✓			
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
```