FortiManager - Release Notes

Version 5.6.1

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 5.6.1 Release Notes
02-561-454506-20180221

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-12-18	Initial release of 5.6.1.
2018-01-18	Added support for FortiOS 5.4.8.
2018-02-21	Added information about upgrading from 5.2.x.

Introduction

This document provides the following information for FortiManager 5.6.1 build 1619:

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

Supported models

FortiManager version 5.6.1 supports the following models:

FortiManager	FMG-200D, FMG-200F, 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 5.6.1

The following is a list of new features and enhancements in 5.6.1. For details, see the *FortiManager Administrator Guide*:

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

Upgrade - One step ADOM upgrade to 5.6.1

One-step procedure to upgrade a 5.4-based ADOM to a 5.6-based ADOM.

FOS-VM HA Cluster Support

FOS-VM HA clusters are now supported by FortiManager. Install and retrieve FOS-VM configurations, authorize UTM services to FOS-VM members, provide metering service for FOS-VM HA cluster and upgrade FOS-VM firmware.

FortiSwitch Manager Improvements

FortiSwitch Manager now supports:

- Trunk interface creation
- DHCP Snooping
- IGMP Network Traffic Snooping
- STP State
- Loop-guard/loop-guard timeout
- Port speed/status

Configurable FortiGuard server location from System Settings

You can now view the list of connected FortiGuard update servers from the *License Information* widget and update the list by selecting a preferred server location.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.6.1.

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 t1sv1
end
```

Port 8443 reserved

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

Upgrade Information

Upgrading to FortiManager 5.6.1

You can upgrade FortiManager 5.4.0 or later directly to 5.6.1. 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 FortiManager 5.4 or 5.6.0 to 5.6.1, it is required to run the following CLI for proper rendering of GUI pages:

```
diagnose cdb upgrade force-retry resync-dbcache
```

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.

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.

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, 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 5.6.1 support

The following table lists 5.6.1 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 57 • Google Chrome version 63 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier	• 5.6.2 to 5.6.3 • 5.6.0 to 5.6.1 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.6.0 and 5.6.1 on page 25. • 5.4.1 to 5.4.8 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.8, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.8 on page 25. • 5.2.8 to 5.2.13 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.10 on page 25. • 5.2.7 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.7 on page 25. • 5.2.6 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.6 on page 26. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.1 on page 26. • 5.2.0 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility issues with FortiOS 5.2.0 on page 26.
FortiAnalyzer	• 5.6.0 to 5.6.1 • 5.4.0 to 5.4.4 • 5.2.0 to 5.2.10 • 5.0.0 to 5.0.13
FortiCache	• 4.2.6 • 4.1.2 • 4.0.0 to 4.0.4
FortiClient	• 5.6.3 • 5.6.0 • 5.4.0 and later • 5.2.0 and later

FortiMail	• 5.4.2 • 5.3.7 • 5.2.9 • 5.1.6 • 5.0.10
FortiSandbox	• 2.5.0 • 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	• 5.8.6 • 5.6.0 • 5.5.4 • 5.4.1 • 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6
FortiDDoS	• 4.4.1 • 4.2.3 • 4.1.11 Limited support. For more information, see Feature support on page 17.

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	✓	✓
Chinese (Simplified)	✓	✓

Language	GUI	Reports
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 5.6.1.

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-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C,FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, **FortiGate 5000 Series:** FG-5001C, FG-5001D **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-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-GCP, 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-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE,FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, 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 3800D, FG-3810D, FG-3815D, FG-3960E, FG3980E, FG-2000E, FG-2500E **FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1 **FortiGate 7000 Series:** FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-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-3815DC **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-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, 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-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM **FortiGate Rugged:** FGR-30D, FGR-30D-ADSL-A, 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-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, 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-800D-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-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-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, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, 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

Model	Firmware Version
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
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
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 5.6.1.

Compatibility issues with FortiOS 5.6.0 and 5.6.1

Bug ID	Description
451036	FortiManager may return verification error on `proxy enable` when installing a policy package.
460639	FortiManager may return verification error on `wtp-profile` when creating a new VDOM.

Compatibility issues with FortiOS 5.4.8

Bug ID	Description
469700	FortiManager is missing three wtp-profiles: FAP221E, FAP222E, and FAP223E.

Compatibility issues with FortiOS 5.2.10

The following table lists interoperability issues that have been identified with FortiManager version 5.6.1 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 5.6.1 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 5.6.1 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 5.6.1 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 5.6.1 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.
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 5.6.1. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
397342	Users may not be able to change the encrypt or disable WiFi broadcast in the AP Manager WiFi templates.
439365	The attribute *Schedule* may be missing in AP Manager SSID configuration.
440650	Users may not be able to configure two DNS servers in SSID profile.
442114	Change of administrative access on WiFi Templates may change the SSID DHCP leasetime.
444739	A newly created WiFi interface may have its role set to undefined by FortiManager.
456043	Users may not be able to add 63 characters long pre-shared key containing a simple or double quotes in SSID WiFi templates.
495156	SSID configuration changes may not trigger config install.

Device Manager

Bug ID	Description
395060	FortiManager may fail to add a v5.6.0 FortiGate LENC device.
397151	Users may be forced to select and admin profile when creating a Restricted Admin to Guest Account Provisioning Only.
399254	Users may see Relay Service from other VDOM's when they are configuring DHCP Server in the Device Manager.
408105	FortiManager may not be able to manage a FortiGate with a long VDOM name.
410995	Users may encounter error popups in the System Interface in CLI-Only pages.
414623	The Change button for host name may be wrongly displayed for FortiGate HA devices.
416266	Changes to the PAC file in *System* > *Explicit Proxy* may not be saved.
416529	`ip-pools` in SSL VPN portal profiles may not be pushed to FortiGate.

Bug ID	Description
417200	`engine-id` under `config system snmp sysinfo` may not be installed to FortiGate.
434847	Users may not be able to select some interfaces in the *Listen on Interfaces for explicit proxy* page in the GUI.
438217	FortiManager may not send Mobile FortiToken activation request.
439546	Users may not be able to deauthorize users from FortiManager.
441237	Users may fail to create a DHCP relay server with a VLAN interface.
441649	Users may fail to enable SNMPv3 in provisioning template for v5.2 ADOMs.
441754	Device revision diff may show passwords 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 in FortiManager under `lte-modem` settings.
442327	FortiManager GUI may show minutes instead of seconds for `webfilter-cache-ttl` and `antispam-cache-ttl` in *Device Manager* > *System* >*FortiGuard*.
445172	Cloned IPSec phase1/phase2 may be missing some configurations.
445688	Retrieving configuration from FortiGate may fail due to duplicate `webfilter url-filter` entries.
446637	Interface attributes `l2forward`, `ipmac` and `subst` may be unset during installation.
447063	Installation may fail if the *md5-key* contains a comma in OSPF settings.
447443	Installing an existing policy package to a new device may cause other devices config status to be shown as *Modified*.
448289	The category Multicast `address6` may not be displayed correctly in import conflicts page.
449225	FortiManager allows users to delete all interfaces of virtual switch.
451737	Adding a FortiGate may fail if there is invalid datasource on the FortiGate.
451796	Upgrade Firmware Task may show *Image upgrade failed* even though it succeeded.
452460	Installation may fail when backslash `\` character is used in the FortiGate username or password.
452616	Users may be able to add a VLAN interface to a FortiGate hardware switch.
452903	Deleting one imported firmware may indeed delete another one other than the selected one.
454254	Device Manager left tree may not be able to display the devices at the very bottom.
455541	*WAN Link Load Balanced* > *Status Check Profiles* may not be configured.
455937	Some VDOMs may be missing.
456713	FortiManager may accept PSK with less than minimum number of characters.

Bug ID	Description
464034	FortiExtender entries may not be displayed.
464244	FortiManager cannot edit settings on the Modem interface.

FortiSwitch Manager

Bug ID	Description
414429	FortiManager may `unset switch-controller` when FortiSwitch is being managed.

Global ADOM

Bug ID	Description
368643	*Find Unused Objects* and *Find Duplicate Objects* tools in Global ADOM may not work.
441162	Deleting an address object from Global ADOM may cause errors when users assign a Global Policy Package.
448616	Deleting a Global policy may not be updated to assigned ADOMs.
451544	Changes in assigned Global Policies may not trigger config status to change to *Modified*.
456046	*Automatically Install Policies to ADOM Devices* may not push Global Policy Packages to all the devices.

Policy and Objects

Bug ID	Description
167355	The default color value of address objects may be different from that on FortiGate.
293781	FortiManager may not support policy hit count reset.
376655	Installation may fail because FortiManager tries to use `net client-cert-request` setting in the `ssl-ssh-profile`.
389768	Traffic shaping policy installations to some FortiGates may fail because of the `config set bandwidth-unit`.
392443	Setting quarantine-expiry for IPS sensor from FortiManager may cause installation to fail.

Bug ID	Description
393077	Setting a global-label for one policy may also apply it to all policies below it.
401482	Exported policies may be missing the column of *Install on scope*.
401843	*Insert policy above/below* may create a duplicate section.
406784	Users may not be able to block the *Unknown Applications* category in Application Control profile from GUI.
411896	Users may not be able to update FSSO correctly from the GUI.
412932	Users may not be able to unset associated interface for a firewall address object from GUI.
416283	Cyrillic letters may not be displayed correctly.
417443	Adding users from *OpenLDAP* and *eDirectory LDAP* may not work.
420104	Users may not be able to see Health Checks in Virtual Servers per-device mappings from GUI.
435971	URL filter rules may be re-ordered following FortiManager upgrade.
438170	When users create custom service and set an `iprange`, `set fqdn` may be used instead of `set iprange`.
438745	Certificate in per device mapping of Virtual Servers may not be saved upon editing.
439086	The sequence number of a policy may be changed after users drag an object to a column.
439356	Not all groups may be displayed when users try to assign a user device to a group.
439594	Users may be unable to delete duplicated dynamic mappings.
440228	Policy packages may not be in an alphabetical order.
440831	Column Filter search in Policy Package may not return the exact matches.
441782	Explicit proxy firewall address groups in object selection may be missing.
442769	Installation Preview may get stuck at 15% following the FortiManager upgrade.
443564	Firewall Policies may not be displayed after they are created.
444304	`server-cert` may not be applied to the `ssl-ssh-profile`.
444316	Importing a Dynamic Mapping of firewall address for a VDOM other than root may fail.
444709	The default HTTPS port number may be 433 in SSL/SSH inspection profile.
445010	LDAP users containing escape characters `\` may not be displayed properly.
445517	Low destination/source port value can be higher than the high destionation/source port.
445651	Users may be able to set multiple `attack_ids` in IPS custom signature.
446026	Policy check process may get stuck at 25%.
446029	*Map to Port* value in VirtualIP objects may be lost after editing.

Bug ID	Description
446245	FortiManager may update the conflicted objects during Import All Objects when users choose *use value from FortiManager*.
447674	The order of custom services may change during policy import.
448113	ADOM revision diff may show that there is difference when two identical revisions.
448459	Some configurations in Web Filter Profiles may not trigger conflict reports during the process of import policy.
448537	Install Wizard may show duplicate occurrence of a device.
449000	Some files may be missing in exported policy package files.
449533	FortiManager may fail to import a URL filter with an apostrophe.
450092	Custom IPS signatures with `!` in the `-pcre` field may not be accepted by FortiManager.
450430	When the last object is removed in a field, it may become empty.
450622	Installation log may show verification errors while the installation has succeeded.
450711	Policy package installation may fail for unset and reset the system resource-limits.
451113	The content in install wizard may be not readable.
451552	Users may receive the error *binding interface does not match dstintf* when they try to delete a source interface.
452022	Policy package status may not change to *Modified* after updating a firewall address object being used in the policy package.
453187	The position indication number shown bottom right may not be accurate.
453329	The UUIDs of cloned objects and policies may be changed on every installation.
453371	After *Object Selector* is set to *Dock to Bottom*, GUI may not be able to render policies on a refresh.
406513	Newly added customer devices in a group may not be installed if they are only used in SSID Exempt list device group.
455627	Users may not be able to create a zone with multiple interfaces.
402174	*Add this user to groups* may be missing in create new LOCAL user page.
436907	The section toggle status may not be remembered.
415338	Object icons may change in policy list unexpectedly.
453436	The empty object selector may be shown after users create a new policy.
459441	Users may need to refresh to see the changes made by drag and drop objects from Object Selector in policy list.
456765	Users may not be able to add custom IPS signatures with `—dns.query_type`.

Bug ID	Description
453942	Policy import may fail because of `server-cert` in the `ssl-ssh-profile` check.
446543	*Block HTTP Redirects by Rating* may not be able to be checked in Web Filter profile.
381161	Duplicate address objects with different comments may be deemed as different.
453744	FortiManager may not check `*` in URL filters in v5.4 ADOMs.
441222	More than 16 ranges may be allowed in service in FortiManager.
371154	In a Policy package re-install, the package selection may change after users do a preview.
435107	FortiManager may install a new Web Filter entry at the end of the Urlfilter table.
448618	Verification may fail when there is Web Filter local rating with a trailing slash created in FortiManager.
452008	Renaming a section may create a new one.
457084	Changing firewall address objects in policy packages may not trigger the Policy Package status to be *Modified*.
457938	`service-group` changes may not get installed to FortiGates.

Script

Bug ID	Description
417075	The *Cancel* button in the run script popup may be misleading.
444976	The *Import Script* function may not be displayed in the top toolkit.

Services

Bug ID	Description
437966	Downstream FortiManager may not receive AV & IPS signatures from Upstream FortiManager.
440718	If an FOSVM joins a HA cluster as a slave when it is in the Unregistered Device List, it may not be able to receive the UTM contract from FortiManager.

System Settings

Bug ID	Description
394218	Admin profiles may not include Global Database in ADOM scope options.
416505	The modules, Policy & Packages, AP Manager and FortiSwtich may not be accessible to Remote Radius admin users.
421868	Users may not be able to delete a v4.3 ADOM.
424389	The fingerprints of certificates may not be displayed.
439377	Duplicate even log entries may be generated for changes made on FortiManager HA master.
443717	Syslog server 1 may be allowed to be deleted.
447281	PKI authentication may not work with mutated vowels in the Subject.
447282	Admin users with *Add/Delete Device Groups* read/write access may not be able to edit Device Groups.
457906	LDAP authentication may fail for group matching issues.

VPN Manager

Bug ID	Description
400529	Changing node settings may not trigger installation when workspace is enabled and installation target is a group.

Workplace and Workflow

Bug ID	Description
423315	The *Save* button may be triggered for a locked policy package.
434642	`execute fmpolicy promote-adom-object` may not work properly in Workflow Mode.
435083	Users are able to quick edit the Comment section without locking the ADOM.
437663	Users may not be able to view objects without locking the ADOM first.

Others

Bug ID	Description
378830	ADOM upgrade from v5.2 to 5.4 may fail because of `DNS-based web-filtering profiles`.
414830	Corrupted images may be accepted for upgrade.
442695	Slave FortiGate may be incorrectly counted as one device for licensing purposes.
452464	There may be too many logs generated for Policy Hit Count.
449964	Switch interfaces created via JSON API may not have a `snmp-index` value.
309449	The ADOM selection upon login may not be remembered.
453579	JSON API may not be able to filter a JASON array using `IN` operator without giving the full list of array values.
453703	Using JSON API to add a device may fail.

Common Vulnerabilities and Exposures

Bug ID	Description
389255	FortiManager 5.6.1 is no longer vulnerable to the following CVE-References: • 2017-9765 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.6.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
464951	Install verification fails when login password is set within an AP profile.
464952	Install verification fails when `fortipresence` is disabled within an AP profile.

Device Manager

Bug ID	Description
456821	After a model device is linked to a real device, VDOMs cannot be displayed.
463164	FortiManager may generate extra interfaces when creating a new ADOM.
460403	FortiManager cannot automatically generate relevant interfaces for VXLANs.
464633	Users cannot double-click to edit VDOM properties.
464607	The CLI-Only settings under `object > system > lte-modem` for FWF-30E cannot be changed. System returns the error: *255 can not be greater than 20*.

Policy & Objects

Bug ID	Description
436852	An object may no longer show up on a policy after renaming the object from the *Object Selector Pane*.
442431	FortiManager returns a runtime error when editing a FSSO agent.
457733	FortiManager does not show default values for anomaly entries within the DoS policy.
462543	FortiManager should not show `null` as the end address for dynamic VIP.

Bug ID	Description
457939	FortiManager should have `ca-cert` set to null when "No certificate" is specified for per-device mapped objects.
460615	Users cannot rename RADIUS server when it is referenced by Authentication within an interface with type set to *Wifi SSID*.
461746	FortiManager is unable to delete IP Pool objects after unchecked *Dynamic IP Pool* within a policy.
463192	FortiManager may take time to edit a firewall policy when database is large.
463847	Multicast address object has associated-interface value set to (null) in device database and "any" in ADOM database resulting in interface binding contradiction error when installing.

Revision History

Bug ID	Description
439512	FortiManager may attempt to delete a RADIUS user group resulting in install failure.
462624	FortiManager may install a policy to all devices even though *Install On* is set to a particular device.
465177	Verification may fail on password attributes when installing a FSSO user.

Script

Bug ID	Description
464786	Run script to create VDOMs may fail.

System Settings

Bug ID	Description
463458	FortiManager may return an empty page when an administrator login profile that has the root ADOM excluded.
462854	The hostname containing the character, `"."`, is not accepted by the *System Information* widget on Dashboard.

VPN Manager

Bug ID	Description
463906	After upgrade, FortiManager should not enable `mode-cfg` when localid is set.

Others

Bug ID	Description
434820	GUI may take several minutes to render a large number of network objects.
460921	FortiManager may not respond promptly when renaming zone via the JSON API.
464103	The JSON API query for getting policy package status may return expected information.

Appendix A - 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	✓	✓		
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
```

Glossary

A

AAA
Authentication, Authorization, and Accounting

AD
Active Directory

ADOM
Administrative Domain

AES
Advanced Encryption Standard

AMI
Amazon Machine Image

AP
Access Point

API
Application Programming Interface

APN
Access Point Name

APT
Advanced Persistent Threat

ATP
Advanced Threat Protection

AV
Antivirus

AVP
Attribute Value Pairs

AWS
Amazon Web Service

B

BGP
Border Gateway Protocol

C

C&C
Command and Control

CA
Certificate Authority

CASI
Cloud Access Security Inspection

CBC
Cipher Block Chaining

CHAP
Challenge-Handshake Authentication Protocol

CIDR
Classless Inter-Domain Routing

CLI
Command Line Interface

CN
Common Name

CoA
Change of Authorization

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSR
Certificate Signing Request

CSV
Comma Separated Value

CVE
Common Vulnerabilities and Exposures

D

DC
Domain Controller, Direct Current

DES
Data Encryption Standard

DH
Diffie-Hellman

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic-Link Library

DLP
Data Loss Prevention

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSRI
Disable Server Response Inspection

DTLS
Datagram Transport Layer Security

E

EA
E-mail Address

EAPOL
Extensible Authentication Protocol over LAN (Local Area Network)

EC
Endpoint Control

EC2
Elastic Compute Cloud

EGP
Exterior Gateway Protocol

EMS
Enterprise Management Server

ESD
Electrostatic Discharge

ESP
Encapsulated Security Payload

F

FAZ
FortiAnalyzer

FCT
FortiClient

FDN
FortiGuard Distribution Network

FDS
FortiGuard Distribution Servers

FG
FortiGate

FGFM
FortiGate-FortiManager

FMG
FortiManager

FQDN
Fully Qualified Domain Name

FSA
FortiSandbox

FSSO
Fortinet Single Sign-On

FTP
File Transfer Protocol

G

GCF
Gatekeeper Confirm

GPRS
General Packet Radio Service

GRE
Generic Routing Encapsulation

GTP
GPRS Tunneling Protocol

GUI
Graphical User Interface

GUID
Globally Unique Identifier

H

HA
High Availability

hcache
Hard Cache

HDD
Hard Disk Drive

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

I

I/O
Input / Output

IBP
Identity-based Policy

ICAP
Internet Content Adaptation Protocol

ICMP
Internet Control Message Protocol

IGP
Interior Gateway Protocol

IKE
Internet Key Exchange

IMAP
Internet Message Access Protocol

IOC
Indicators of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

ISDB
Internet Service Database

ISP
Internet Service Provider

IV
Initialization Vector

J

JSON
JavaScript Object Notation

L

L2TP
Layer 2 Tunneling Protocol

LACP
Link Aggregation Control Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

MD5
Message Digest 5

MGCP
Media Gateway Controller Protocol

MIB
Management Information Base

MMC
Microsoft Management Console

MSCHAP
Microsoft Challenge-Handshake Authentication Protocol

MSS
Maximum Segment Size

N

NAC
Network Access Control or Compliance

NAS
Network Access Server

NAT
Network Address Translation

NAT-PT
Network Address Translation (NAT) Port Translation

NDcPP
Network Device Collaborative Protection Profile

NGFW
Next-Generation Firewall

NNTP
Network News Transfer Protocol

NOC
Network Operations Center

NPU
Network Processing Unit

NTLM
NT LAN Manager

NTP
Network Time Protocol

O

OCSP
Online Certificate Status Protocol

OFTP
Odette File Transfer Protocol

ONC-RPC
Open Network Computing Remote Procedure Call

OSPF
Open Shortest Path First

OTP
One-time Password

OU
Organization Unit

OUI
Organizationally Unique Identifier

OVF
Open Virtualization Format

P

PAP
Password Authentication Protocol

PAT
Port Address Translation

PEM
Power Entry Module

PFS
Perfect Forward Secrecy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PoE
Power over Ethernet

POP3
Post Office Protocol 3

PPP
Point-to-Point Protocol

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

R

RADIUS
Remote Authentication Dial-In User

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Registration, Admission, and Status

RBAC
Role Based Access Control

RCF
Registration Confirm

RDP
Remote Desktop Protocol

REST
Representational State Transfer

RFC
Remote Function Call

RSH
Remote Shell

RSSO
RADIUS Single Sign-On

RTM
Real-Time Monitor

RTP
Real-Time Protection

RTSP
Real-Time Streaming Protocol

S

SAN
Storage Area Network

SAP
Shelf Alarm Panel

SCEP
Simple Certificate Enrollment Protocol

SCP
Secure Copy

SCVP
Server-based Certificate Validation Protocol

SDK
Software Development Kit

SDN
Software-Defined Networking

SFTP
Secure (or SSH) File Transfer Protocol

SHA1
Secure Hash Algorithm 1

SIP
Session Initiation Protocol

SMTP
Simple Mail Transfer Protocol

SNAT
Secure Network Address Translation

SNI
Server Name Indication

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SQL
Structured Query Language

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

T

TACACS+
Terminal Access Controller Access-Control System

Tcl
Tool Command Language

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TNS
Transparent Network Substrate

TTL
Time-to-live

U

UDP
User Datagram Protocol

UID
Unique Identifier

URI
Uniform Resource Identifier

URL
Uniform Resource Locator

UTM
Unified Threat Management

UUID
Universally Unique Identifier

V

VDOM
Virtual Domain

VHD
Virtual Hard Disk

VIP
Virtual Internet Protocol

VLAN
Virtual Local Area Network

VM
Virtual Machine

VMDK
Virtual Machine Disk

VoIP
Voice over Internet Protocol

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VSA
Vendor Specific Attribute

W

WAF
Web Application Firewall

WAN
Wide Area Network

WCCP
Web Cache Communication Protocol

WIDS
Wireless Intrusion Detection System

WPA
Wi-Fi Protected Access

WPA2
Wi-Fi Protected Access II

WSDL
Web Services Description Language

WTP
Wireless Transaction Protocol

X

XAuth
Extended Authentication

XML
eXtensible Markup Language

XSS
Cross-site Scripting

XVA
XenServer Virtual Appliance

Index

L

O

P

Q

S

V

X