FortiManager - Release Notes

Version 6.0.5

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 24, 2020
FortiManager 6.0.5 Release Notes
02-605-555292-20200424

TABLE OF CONTENTS

FortiManager 6.0.5 Release

This document provides information about FortiManager version 6.0.5 build 346.

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

This section includes the following topics:

Supported models

FortiManager version 6.0.5 supports the following models:

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

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.0.5.

Configuration changes to FQDN addresses after upgrade

After upgrading both FortiManager and FortiOS from 6.0.4 to 6.0.5, the configuration changes for some of the default FQDN addresses that have been moved under *Wildcard FQDN* addresses. To avoid a conflict that causes installation failure, rename the affected addresses, for example, `google-play` changes to `fqdn_google-play` after upgrading to 6.0.5.

Workaround:

1. Retrieve the configuration on the affected FortiGate.
2. Run a script on the policy package or ADOM database for the affected addresses:

```
config firewall address
rename "swscan.apple.com" to "fqdn_swscan.apple.com"
rename "update.microsoft.com" to "fqdn_update.microsoft.com"
rename "google-play" to "fqdn_google-play"
rename "autoupdate.opera.com" to "fqdn_autoupdate.opera.com"
end
```

Managing FortiGate with VDOMs that use Global Profiles

Because of changes made to FortiOS 6.0.0 and later, FortiGate units with VDOMs enabled that are running FortiOS 6.0.0 and later cannot be successfully added to FortiManager without a workaround. Before adding the FortiGate units to FortiManager, perform the following steps to unset default configurations. After the default configurations are unset, you can successfully add the FortiGate units to FortiManager.

1. On the Fortigate for each VDOM, unset the following default configurations by using the CLI:

```
config wireless-controller utm-profile
    edit "wifi-default"
        set comment "Default configuration for offloading WiFi traffic."
    next
    edit "g-wifi-default"
        set comment "Default configuration for offloading WiFi traffic."
        set ips-sensor "g-wifi-default"
        set application-list "g-wifi-default"
        set antivirus-profile "g-wifi-default"
        set webfilter-profile "g-wifi-default"
        set firewall-profile-protocol-options "g-wifi-default"
        set firewall-ssl-ssh-profile "g-wifi-default"
    next
```

```
end

FGVMULCV30310000 (utm-profile) # ed g-wifi-default

FGVMULCV30310000 (g-wifi-default) # unset ips-sensor

FGVMULCV30310000 (g-wifi-default) # unset application-list

FGVMULCV30310000 (g-wifi-default) # unset antivirus-profile

FGVMULCV30310000 (g-wifi-default) # unset webfilter-profile

FGVMULCV30310000 (g-wifi-default) # unset firewall-profile-protocol-options

FGVMULCV30310000 (g-wifi-default) # unset firewall-ssl-ssh-profile

FGVMULCV30310000 (g-wifi-default) # sh
config wireless-controller utm-profile
    edit "g-wifi-default"
        set comment "Default configuration for offloading WiFi traffic."
    next
end
```

2. After the default configurations are unset, you can add the FortiGate unit to FortiManager.

IOC Support on FortiManager

Please note that FortiManager does not support IOC related features even when FortiAnalyzer mode is enabled.

FortiManager 6.0.2 support for FortiOS 6.0.3

FortiManager 6.0.2 treats the `status` field of firewall policies as a mandatory field, and it is set to `enable` by default. FortiOS 6.0.3 has reverted this change. As a result, FortiManager may report verification failures on installations. The verification report shows that the policy `status` field has to be installed with the `enable` setting:

```
"---> generating verification report
   (vdom root: firewall policy 1:status)
   remote original:
   to be installed: enable

<--- done generating verification report


install failed"
```

Reconfigure SD-WAN after Upgrade

The SD-WAN module has been fully redesigned in FortiManager v6.0 to provide granular monitor and control. Upgrading SD-WAN settings from 5.6 to 6.0 is not supported. Please reconfigure SD-WAN after upgraded to v6.0.

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.

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.

Recreate Guest List for Guest user group

After upgrading to FortiManager 6.0.3, recreate the guest list for the *Guest* user group in ADOM Policy Object before installing device settings to FortiGate devices. For more information, see Bug ID 499568 in *Resolved Issues*.

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.

SSLv3 on FortiManager-VM64-AWS

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

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

Upgrade Information

You can upgrade FortiManager 5.6.0 or later directly to 6.0.5. If you are upgrading from versions earlier than 5.6.x, you should upgrade to the latest patch version of FortiManager 5.6, then 6.0.0.

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

This section contains the following topics:

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}
```

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*.

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.

Aliyun

- `.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.

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 FortiManager 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.

Google GCP

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

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.

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

This section lists FortiManager 6.0.5 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

FortiManager 6.0.5 support

The following table lists 6.0.5 product integration and support information:

Web Browsers	• Microsoft Edge 40 Due to limitation on Edge, it may not completely render a page with a large set of policies or objects. • Mozilla Firefox version 66 • Google Chrome version 74 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 6.0.0 to 6.0.5 • 5.6.5 to 5.6.8 • 5.6.4 FortiManager 5.6.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.4, with some minor interoperability issues. For information, see FortiOS 5.6.4 compatibility issues on page 26. • 5.6.2 to 5.6.3 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.2 to 5.6.3, with some minor interoperability issues. For information, see FortiOS 5.6.3 compatibility issues on page 26. • 5.6.0 to 5.6.1 FortiManager 5.6.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.0 to 5.6.1, with some minor interoperability issues. For information, see FortiOS 5.6.0 and 5.6.1 compatibility issues on page 27. • 5.4.10 FortiManager 5.4.5 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.10, with some minor interoperability issues. For information, see FortiOS 5.4.10 compatibility issues on page 27. • 5.4.9

	FortiManager 5.6.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.9, with some minor interoperability issues. For information, see FortiOS 5.4.9 compatibility issues on page 27. • 5.4.1 to 5.4.8 • 5.2.8 to 5.2.13 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see FortiOS 5.2.10 compatibility issues on page 28. • 5.2.7 FortiManager 5.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see FortiOS 5.2.7 compatibility issues on page 28. • 5.2.6 FortiManager 5.2.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see FortiOS 5.2.6 compatibility issues on page 28. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.2.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see FortiOS 5.2.1 compatibility issues on page 28. • 5.2.0 FortiManager 5.2.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see FortiOS 5.2.0 compatibility issues on page 29.
FortiAnalyzer	• 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.0 and later
FortiAuthenticator	• 5.0 to 5.5 • 4.0 to 4.3
FortiCache	• 4.2.9 • 4.2.6 • 4.1.2 • 4.0.0 to 4.0.4
FortiClient	• 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later
FortiMail	• 5.4.9 • 5.3.13 • 5.2.10 • 5.1.7

	• 5.0.10
FortiSandbox	• 2.5.0 to 2.5.2 • 2.4.0 and 2.4.1 • 2.3.2 and 2.3.3 • 2.2.2 • 2.1.3 • 1.4.0 and later • 1.3.0 • 1.2.0 and later
FortiSwitch ATCA	• 5.2.3 • 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 6.0.4 • 5.9.1 • 5.8.6 • 5.8.3 • 5.8.1 • 5.8.0 • 5.7.2 • 5.6.1 • 5.5.6 • 5.4.1 • 5.3.9 • 5.2.4 • 5.1.4 • 5.0.6
FortiDDoS	• 4.5.0 • 4.4.1 • 4.2.3 • 4.1.11 Limited support. For more information, see Feature support on page 16.
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 7.2 • Linux KVM Redhat 7.1 • Microsoft Azure • Microsoft Hyper-V Server 2012 and 2016 • OpenSource XenServer 4.2.5 • VMware ESXi versions 5.0, 5.5, 6.0, 6.5 and 6.7

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			✓	✓
FortiAuthenticator				✓
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)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓

Language	GUI	Reports
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 create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide.*

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.0.5.

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.

This section contains the following topics:

FortiGate models

Model	Firmware Version
FortiGate: FGT-30E-3G4G-GBL, FGT-3400E, FGT-3401E, FGT-3600E, FGT-3601E, FGT-400E, FGT-401E, FGT-600E, FGT-601E, FGT-100F, FGT-60E-DSL, FGT-60E-DSLJ, FWF-60E-DSL, FWF-60E-DSLJ, FGT-VM64-RAXONDEMAND, 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-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-100F, FG-101E, FG-101F, 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, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **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:** FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, 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-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP,VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0
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-60E-DSL, 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, FG-5001E, FG-5001E1 **FortiGate 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiGate 7000 Series:** FG-7030E, FG-7040E, FG-7060E	5.6

Model	Firmware Version
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, FG-7060E-8-DC **FortiGate Hardware Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **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-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	
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 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **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, FG-7060E-8-DC **FortiGate Hardware Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **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: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001C, FGT-5001D, FGT-5001E **FortiCarrier 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E	5.6

Model	Firmware Version
FortiCarrier-DC: FGT-3000D-DC, FGC-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FCR-3810D-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E **FortiCarrier 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E **FortiCarrier-DC:** FGT-3000D-DC, FGC-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FCR-3810D-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.4
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, , FGT-3810A, FGT-3810D, FGT-3950B, FGT-3951B, FGT-5100B, FGT-5100C, FGT-5001D, FGT-5101C, FS-5203B, FT-5902D **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3810A-DC, FGT-3810D-DC, FGT-3950B-DC, FGT-3951B-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-Xen	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-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4.5
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	5.3.12
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	5.2.10
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	5.1.7
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-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.3
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.3 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ATCA models

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

FortiSwitch models

Model	Firmware Version
FortiSwitch: FortiSwitch-108D-POE, FortiSwitch-108D-VM, FortiSwitch-108E, FortiSwitch-108E-POE, FortiSwitch-108E-FPOE, FortiSwitchRugged-112D-POE, FortiSwitch-124D, FortiSwitch-124D-POE, FortiSwitchRugged-124D, FortiSwitch-124E, FortiSwitch-124E-POE, FortiSwitch-124E-FPOE, FortiSwitch-224D-POE, FortiSwitch-224D-FPOE, FortiSwitch-224E, FortiSwitch-224E-POE, FortiSwitch-224E-FPOE, FortiSwitch-248D, FortiSwitch-248D-POE, FortiSwitch-248D-FPOE, FortiSwitch-248E-POE, FortiSwitch-248E-FPOE, FortiSwitch-424D, FortiSwitch-424D-POE , FortiSwitch-424D-FPOE, FortiSwitch-448D, FortiSwitch-448D-POE, FortiSwitch-448D-FPOE, FortiSwitch-524D, FortiSwitch-524D-FPOE, FortiSwitch-548D, FortiSwitch-548D-FPOE, FortiSwitch-1024D, FortiSwitch-1048D, FortiSwitch-1048E, FortiSwitch-3032D, FortiSwitch-3632D	N/A There is no fixed supported firmware versions. If FortiGate supports it, FortiManager will support it.

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
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	5.5.6
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

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.9
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

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E **FortiProxy VM:** FPX-KVM, FPX-VM64	1.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.3 and 5.0-5.3
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.0-4.2

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.0.5. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 5.6.4 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 5.6.3 and FortiOS 5.6.4.

Bug ID	Description
486921	FortiManager may not be able to support the syntax for the following objects: • `rsso-endpoint-block-attribute`, `rsso-endpoint-block-attribute`, or `sso-attribute` for RADIUS users. • `sdn` and its `filter` attributes for firewall address objects. • `azure` SDN connector type. • `ca-cert` attribute for LDAP users.

FortiOS 5.6.3 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 5.6.1 and FortiOS 5.6.3.

Bug ID	Description
469993	FortiManager has a different default value for switch-controller-dhcp-snooping from that on FortiGate.

FortiOS 5.6.0 and 5.6.1 compatibility issues

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

FortiOS 5.4.10 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 5.4.5 and FortiOS 5.4.10.

Bug ID	Description
508337	FortiManager cannot edit the following configurations for replacement message: • `system replacemsg mail "email-decompress-limit"` • `system replacemsg mail "smtp-decompress-limit"` • `system replacemsg nntp "email-decompress-limit"`

FortiOS 5.4.9 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 5.6.3 and FortiOS 5.4.9.

Bug ID	Description

486592	FortiManager may report verification failure on the following attributes for RADIUS users:
	`rsso-endpoint-attribute`
	`rsso-endpoint-block-attribute`
	`sso-attribute`

FortiOS 5.2.10 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 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.

FortiOS 5.2.7 compatibility issues

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

FortiOS 5.2.6 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 5.2.4 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.

FortiOS 5.2.1 compatibility issues

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

FortiOS 5.2.0 compatibility issues

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

Resolved Issues

The following issues have been fixed in 6.0.5. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
403766	Firmware upgrade task was stuck in that state for more than 2 hours.
436774	FortiManager is missing permission settings when managing FortiAnalyzer.
443240	HA-status changes to standalone from ELBC cluster when making changes to FortiGuard server setting directly on FortiGate.
460615	FortiManager should adjust Radius configuration on SSID when renaming a Radius server.
474245	The "set disk-usage log" command should not be installed for devices with log disk.
489373	Passwords should allow special characters on certificate templates in FortiManager.
492088	FortiManager attempts to change Chassis ID on FortiGate 7000 series when installing configuration.
497900	User cannot paste password in managed device's Telnet or SSH console.
498107	When an address is a member of a dynamic address group, its "Where Used" results does not say which dynamic group it belongs.
500037	FortiToken provision does not work.
502882	Operator to filter Event logs on FortiManager may not work properly.
502945	FortiManager returns TCL Error when pushing Policy to FortiGate due to failure to resolve hostname defined under "set fmg".
503722	FortiSwitch Manager and AP Manager reports switches and APs connected to FortiGates as online when the devices are no longer powered on.
504962	When creating new vdom-link from the global interface menu, all the VDOMs should be visible in the management VDOM.
507044	FortiManager always overrides the device-level configured parameters to DPD 'default values' making impossible to tune DPD settings when using VPN Manager.
507231	FortiManager pushes IP POOL with pool type not specified but with parameter "set num-blocks-per-user 32" set.
508340	With the ADOM option "Perform Policy Check Before Every Install" enabled and no changes to install, an install will fail with the "Validation Failed" message.
511826	FortiManager should remove the mandatory requirement of having a hub-to-hub interface when two hubs are defined in a VPN community using VPN Manager.
512046	When workspace is enabled, IPv6 session based counters are synchronized with FortiGate.

Bug ID	Description
515101	Admin users are unable to login from the GUI when their password contains two sequential question marks.
517061	ADOM upgrade may fail when the IPs in FortiSwitch VLAN DHCP server are configured with zero.
517376	*FortiSwitch Manager* > *FortiSwitch Templates* > *FortiSwitch VLANs* missing advanced options.
518351	During import, FortiManager does not checking if adding suffix to object name will exceed character limit.
519422	Deleting multiple SD-WAN rules does not work.
519484	DHCP Gateway option may not working in AP Manager.
519495	Running a script always returns the error, 'the script is not eligible', even though the actual error may be different.
520651	When querying a policy package, FortiManager API's response may be missing the VDOM information.
520691	FortiManager should warn user in install wizard if there is an IP address being installed that is 0.0.0.0/0.
520964	FortiManager is not able to assign FQDN address object to Static Route Named Address.
521063	FortiManager responses with errors if multiple protected subnets are defined in Dial-Up community external spoke configuration.
521649	Policy counters may not be accurately synchronized with the FortiGate devices.
521900	SD-WAN rule protocol options 'ANY' is not saved on GUI.
521905	Tooltip for device lock is not show in Device Manger's device tree.
522070	Right-click menu does not allow firmware upgrade with device locked.
522206	GTP global tunnel limit is not configurable on FortiManager.
522456	FortiManager does not support the increased firewall addresses limit to 10000 objects for FGT81E or FGT81_POE.
522713	ADOM upgrade stuck at 5%.
522828	FortiManager unsets `dhcp-snooping` when installing from a 5.4 ADOM.
523208	FortiManager is trying to unset the category for user device when pushing policy package.
523228	Search in zone does not work after upgrade.
523480	IPS Filter does not include ALL if filtered based on OS.
523649	FortiManager is not updating the last modified time when modifying a web filter category.
523705	In web filter profile, FortiManager should only allow configuring quota for categories set to monitor, warning, or authenticate.
523712	FortiManager may attempt to add trailing spaces for VIP's mapped IP.
523817	Push update should be available from Manager > License.

Bug ID	Description
524447	Editing SD-WAN interface shows inaccurate GUI Page.
524607	FortiManager should not allow illegal change with `ssl-ssh-profile` causing installation to fail.
524684	API request returns all the devices even when the user does not have access to other ADOMs.
525231	When adding a system administrator, the Virtual Domain field is missing when the option, "Match a user on remote server group/Match all users on remote server " is selected.
525646	FortiManager cannot delete WF and AS FortiGuard databases on FortiManager.
525926	The Local Users column is always empty even if a token is assigned.
525927	*Import all objects* is not importing unused FortiTokens.
525928	Token used in device local admin configuration is displayed as not used at ADOM level.
526002	When having multiple hosts within an SNMP community, it is not possible to edit a host and change the status of HA-direct.
526232	The `execute reset hitcount` command tries to reset on v5.2 ADOMs, which have no hitcounts feature resulting system returning failure with code -160
526287	Policy install may stuck at 67%.
526642	Some SMTP/splice options under firewall profile-protocol options cannot be disabled.
526935	List of static route is always empty if user uses search filter before edit or clone a static route.
527140	FortiManager is unable to add multiple DHCP Relay Servers from the Device Manager System Interface Menu.
527407	Users may not be able to change the FortiGate HA management interface IP.
527650	Importing a local certificate with a big number of subject alternative names is not supported.
528633	IS-IS interfaces cannot be deleted from GUI.
528916	Users may not be able to upgrade ADOM after ADOM name has been changed.
528931	FOS-VM may be getting invalid license from FMGR-VM-Meter.
528938	FortiManager does not allow users to manually set SD-WAN member sequence ID.
528977	FortiGuard 7000 Service Status shows slave chassis with serial number instead of host name.
529036	VPN Manager should not show the options for main and aggressive mode when IKEv2 is selected.
529045	FortiManager should not prompt for Device setting for static route in TP VDOM.
529475	Web filter and Application profiles are not available in the FortiClient profile GUI.
529771	Upgrading ADOM 5.2 to 5.4 may be very timing consuming.
530207	Installing configuration after fail-over in cluster causes installation fail because of difference in management-ip.
530249	Policies that are *Last Modified* matched by actual traffic always shows recently modified by 'admin'

Bug ID	Description
	even if the default admin user is not present in the FortiManager configuration.
530376	Users are unable to select Schedule Object for SSID in AP Manager.
530498	Read-Only admin can enable VPN Manager in the ADOM.
530735	FortiManager may not be able to configure a full-mesh VPN among FortiGates with multi-VDOMs.
530749	FortiManager is unable to import policy configuration from devices with a long VDOM name.
530792	When configuring Per-Device Mappings for Real Servers, mode is missing and users cannot create multiple real servers.
530837	Users should not be allowed to delete default Meta fields.
531338	Column showing unused object reverts to original size after scrolling down.
531489	Re-importing a device may result in policy package status change to "modified" for many devices.
531508	When trying to add a new gateway from VPN Manager, FortiManager returns an error 'peer invalid value'.
531573	FortiManager is not able to set Type of Service field for SD-WAN service.
531610	FortiManager is showing 'Create New' option under script even though ADOM is not locked.
531645	FortiManager should be able to configure dynamic mappings for SD-WAN via a script.
531813	With Safari, there are two issues when user editing device group: there are two scrollbars in the "Edit Device Group" window and "Edit Device Group" window size cannot be changed.
531826	Duplicated section title name issue in policy packages.
531963	SSL/SSH Profile should not allow the user to enable "Allow Invalid SSL Certificates" when Inspection mode is "SSL Certificate Inspection".
532075	When editing comment/description, FortiManager may display the slash character, “/”, as “&#x2F”.
532275	*Device Manager* > *System Admin Profile*: Unable to change Access control due to JavaScript error.
532488	Bytes/Hit/packet count should not be a parameter to consider in the Diff as these are not part of configuration.
532721	Once a Local ID value is configured for a VPN Node within VPN Manager, it can no longer be removed.
532943	FortiGate's system time is now shown on FortiManager when time zone index is set at 79, 80, or 83.
533141	Retrieving configuration under Workspace mode does not allow further changes under AP manager.
533213	FortiManager should support encrypted disk on AWS Cloud.
533857	FortiManager is unable to automatically register devices via Pre-Shared Key method if a revision is imported prior to registering the devices.

Bug ID	Description
534173	FGFM debug shows `fgfm_keepalive_handler` entries for all managed devices in fgfm debug output when device filter is specified.
534188	FortiManager is unable to import 7040E v5.6.
534559	Editing Wi-Fi interface, which is a zone member, should not enable block intra-zone traffic.
534784	FSSO Agent with option *Select FSSO groups via FortiGate* does not work if the policy has no pending changes.
534927	When there is a dynamic interface and a multicast interface that has the same name within a policy package, the install wizard was not be able to create dynamic mappings.
535170	FortiManager does not accept FQDN address configuration containing the _ character.
535245	After upgrade, install may fail due to invalid VDOM snmp-index.
535525	Dynamic/Dialup Type IPSec Tunnel Interface cannot be added as SD-WAN member.
535621	Retrieving or importing configuration revision fails if configuration contains a large number of CRLs.
535743	Downstream FortiManager does not update Signature until changing schedule setting in the second tier FortiManager's FDN.
536043	When ADOM is locked, FortiManager may display incorrect values or configurations from some objects or policies.
536113	AP Manager may not be able to change wtp-mode.
536805	Install fails for DoS policy quarantine-expiry.
537135	There is no GUI validation when an invalid subnet mask is used as destination for a Static Route.
537197	Change to policy with install target specified should not change the status of ALL targets within the policy package.
537214	The command, execute device replace, is missing username.
537236	LDAP query failure over slow satellite connection.
537752	FortiManager tries to add full scan options while using quick scan in default AV profile.
537775	Proxy policy should not allow empty source address.
538029	Occasionally, duplicate sequence number may appear in some policy packages.
538934	Install to device may delete configuration on FortiGate cluster with large configuration file.
539184	FortiManager should not install forward-error-correction on VLANs.
539197	The "Policy Package" column is missing in "Where Used" result after upgrade.
539998	Install fails when deny rule contains DNS filter profile.
540065	FortiManager should be able to display CA certificate under 6.0 ADOM.
540095	Scheduled TCL Script intermittently fails to run on the scheduled time after upgrade.

Bug ID	Description
540222	Policy package status changed to "Never Installed" after upgrade.
540657	There is an ordering issue on admin users where multiple wildcard users are configured on the same server.
540936	Remote wildcard users breaks user profile access to workflow sessions.
541015	FortiManager may not be able to configure or import IPS custom signature.
542024	Where Used may not point to the entity using the object.
542472	Adding section for traffic shaping policies causes runtime error.
542823	Script fails to set `accprofile` on device database.
543129	User may not be able to delete ADOM from Global Assignment.
543251	Policy Package name is truncated in table with "Where Used" output.
543567	FortiManager does not install new certificate obtained from FortiAuthenticator.
543734	Key Type specified, as elliptic curve is not functional when generating a CSR.
544121	Installation log is missing due to `dpm-logsize` limited to 10MB.
544142	Installation fails due to DNS server "Same as Interface IP" option inside device interface configuration.
544580	Two SSL-SSH profiles added by FortiManager may cause installation issue.
544886	When importing device list of multiple model devices with PSKs, FortiManager prompts the error, "Serial number already in use".
545143	Adding wildcard FQDN for SSL inspection exemption list from FortiManager fails.
545457	AP Manager may not be able to show map.
545480	When attempting to remove a VDOM from a FortiGate by running a script, the script fails unexpectedly and the VDOM is not deleted.
545491	FortiManager may fail to retrieve configuration when there are more than 10000 central NAT entries.
545813	Users may not be able to see SD-WAN options in Backup mode after switching from Normal mode.
547646	FortiManager should not push ssh-filter profile `upgrade_1` to FortiGate devices after upgrade.
547740	When FortiManager is running in workspace mode, FortiManager may unexpectedly delete firewall policy.
548320	User should be able to create a FortiGate admin account with *Restrict Admin to Guest Account Provisioning Only* option selected with VDOM(s) guest group(s).
548416	Changes on Existing Static Route is not displayed on Installation Preview.
550240	FortiGuard service event logs should always been generated with an internal FortiManager user.

Bug ID	Description
551057	FortiManager does not give an option to choose RSA 4096 and Elliptic Curve algorithms in certificates.
552069	FortiManager may fail to install local certificate on FortiGate and private key is missing after saving the configuration.

Known Issues

The following issues have been identified in 6.0.5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
540347	FortiManager has no option available to configure VLAN IDs under VLAN Pooling.
547361	AP Profile in AP Manager may offer redundant options for specific AP models which can lead to failed installation.
548329	*WiFi Profiles SSID DHCP Server* Toolbar is hidden if *System Settings* is set to *None* in an Admin Profile.
549001	Installation error after changing inspection mode from Proxy to Flow.
549113	In case FortiGate is in NGFW policy-based mode, URL or Application control profiles should not be visible on FortiManager.
549615	Users should be able to set the `login-timestamp` from CLI script.
549638	MAC address Access control list entries under DHCP server are duplicated when editing one of the entries.
549674	FortiManager is unable to create SD-WAN Template in Central Management Mode if System Settings is set to *None* in an Admin Profile.
550513	User cannot change IPSec Phase1 on an existing IPSec Phase2 interface.
551072	Assignment of `object-tag` from 5.6 Global ADOM to 6.0 ADOM should not fail.
551077	FortiManager may not be able to import policies from FortiGate SLBC.
551237	User without Super User Profile is unable to manage Tags from Tag Management.
551701	FortiManager is unable to Set OSPF Interface Network Type as *P2MP*.
552110	FortiManager cannot show *where used* for FortiSwitch Security Policy.
552144	Install copy fails when setting captive portal user group for FortiSwitch's VLAN.
553270	Imported SSIDs cannot be selected within AP Profile until the SSIDs have been edited.
553276	When SSID is in bridge mode, external link to captive portal and CMCC Radius Secret are missing on AP Manager's SSID page.
553704	*Find Duplicate Objects* may get stuck loading.
553860	FortiManager should have public IP for `remote-gw` under IPSec Phase1 interface.
553926	Split-tunneling information may not be retrieved completely for managed AP.
553933	User should be able to configure split-tunneling related information on AP profile and managed AP pages.

Bug ID	Description
553985	FortiManager incorrectly sets `security-external-web` when external authentication is selected.
553991	When *redirect after captive portal* is set, verification may fail on `security-redirect-url` due to missing http:// prefix.
554001	Configuration may modify FQDN addresses after FortiManager and FortiGate are both upgrade to version 6.0.5.
554092	FortiManager is unable to use interface member of a zone as *Source Interface* filter for VIP object.
554154	FortiManager is unable to select multiple FortiExtender units for upgrade of firmware from *Extender* tab.
554491	Device Manager generates incorrect configuration for Filter MAC Addresses on SSID that causes installation to fail.
554500	Device Manager's SSID page cannot save links to authentication portal and redirect after captive capital.
554761	FortiManager is missing to generate software switch related configurations for Quarantine Host for SSID.
554778	AP Manager may not be able to import AP Profile for FAP-421E/423E/S421E/S423E.
554882	7000 series HA members may show up as unregistered after failover.
554901	EU country ID is available on FortiManager, but the ID is not part of latest geographic database.
554946	Sub-admin clicks *View on where Used* may lead to disappearance of dual panel.
555159	After deleting an SSID from Device Manager, AP Manager still shows the SSID.
555257	Search box for SSID selection within AP Profile may not work well.
555730	Install may fail if zone member is used in a Multicast policy.
556192	Resetting hitcount in ADOM 5.4 fails.
556192	FortiManager may fail to run `execute fips kat all` and `diagnose system fips kat-error` commands.
556368	FortiManager may show Device objects from another ADOM.
558445	Per-Device mapping function may not be available for SD-WAN interface member. Workaround: Configure per-device mappings via CLI script.
558482	FortiManager may not be able to create a LDAP user.
560332	Some CLI widgets are not available in the root ADOM when using multiple wildcard accounts. The error *Non-root ADOM user cannot access CLI* is shown.

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	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Windows)	✓		✓	
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			

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
```

Change Log

Date	Change Description
2019-05-14	Initial release of 6.0.5.
2019-05-15	Added FortiGate models for 6.0. Added 554001 to *Known Issues*.
2019-05-17	Removed Microsoft Internet Explorer 11 from *Product Integration*. Added 558482 and 558445 to *Known Issues*.
2019-05-21	Added FMG-1000F to *Supported Models*.
2019-05-27	Added a special notice. Added 525231 to Resolved Issues.
2019-05-29	Added hyphens to FortiGate models for consistency.
2019-06-10	Added 560332 to *Known Issues*.
2019-07-02	Added 403766 to *Resolved Issues*.
2019-08-01	Added FGT-100F to *FortiGate models*.
2019-09-17	Added a special notice.
2019-11-27	Added 531826 to *Resolved Issues*.
2020-04-24	Added *Configuration changes to FQDN addresses after upgrade* to *Special Notices*.