FortiManager Release Notes

VERSION 5.2.6

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

October 3, 2016

FortiManager 5.2.6 Release Notes

02-526-363458-20161003

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-03-17	Initial release.
2016-03-21	Updated FortiGate supported models; added special notice "Limitation on backing up and restoring FortiManager's Database"; added known issue 294021 and 305369.
2016-03-31	Added known issue 365412 and 365743; added support for FortiOS/FortiOS Carrier 5.2.7 and compatibility issues.
2016-10-03	Added 356873 to Resolved Issues.

Introduction

This document provides the following information for FortiManager 5.2.6 build 753:

- Supported models
- Special Notices
- Upgrade Information
- Product Integration and Support
- Compatibility with FortiOS Versions
- Resolved Issues
- Known Issues
- FortiGuard Distribution Servers (FDS)

For more information on upgrading your device, see the FortiManager 5.2.6 Upgrade Guide.

FortiManager 5.2.6 is the immediate next version of FortiManager 5.2.4. There is no FortiManager 5.2.5.

Supported models

FortiManager version 5.2.6 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG64-AWS, and FMG-VM64-HV.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.2.6.

Limitation on backing up and restoring FortiManager's Database

Users may not be able to back up and restore FortiManager's database from web GUI when the backup file is 2 GB or larger. For large scale deployments, please back up FortiManager's database via CLI with FTP, SCP, or SFTP.

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.

Multicast Policy Support at ADOM Level

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

ADOM for FortiGate 4.2 Devices

FortiManager 5.2 no longer supports FortiGate 4.2 devices. FortiManager cannot manage the devices after the upgrade. To continue managing those devices, please upgrade all FortiGate 4.2 devices 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 FortiAnalyzer-VM64-AWS

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

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

SQL database rebuild

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

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

Web Portal support

Web Portal is no longer available as it has been replaced by Restricted Admin Profile in version 5.2. Users can still access web portal content via the Web Portal API services.

CLI commands for configuring dynamic objects

In version 5.2, all dynamic objects are consolidated from devices to the ADOM database. For those users who wish to configure a dynamic mapping via a CLI script, the configuration for the mapping must be defined in the dynamic object under the `config dynamic_mapping` sub-tree. Also, the CLI script must be run on policy package instead of the device database. Below are some examples:

Example 1: Dynamic VIP

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

Example 2: Dynamic Address

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

Example 3: Dynamic Interface

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

FortiManager VM

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

FortiAnalyzer feature set

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

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

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

The FortiAnalyzer feature set is not available on the FMG-100C.

In version 5.2.6, you can enable the FortiAnalyzer feature set in the Web-based Manager. Go to *System Settings* > *Dashboard*. In the *System Information* widget, beside *FortiAnalyzer* Features, select *Enabled*.

FortiGate firmware upgrade

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

System time on FortiManager VM

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

Memory requirement for FortiManager VM64-HV

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

ADOM for FortiCarrier

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

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

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

FortiOS 5.0 override server setting for FortiGuard Services

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

This is applicable to FortiOS version 5.0 only. FortiOS version 4.3 and 5.2 have different behaviors.

Ports used by FortiGuard services

Port	Service
8890	Antivirus or IPS updates for FortiGate

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

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

Example 1: Antivirus/IPS

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

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

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

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

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

Example 2: Web filtering/Antispam

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

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

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

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

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

Update services provided to FortiMail 4.2 devices

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

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

Endpoint management

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

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

FortiManager VM license check

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

Multi-language display support

FortiManager version 5.2.0 or later has restrictions on supporting a FortiGate device's multi-language display.

Importing a FortiManager generated policy

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

- Global Header Policy
- Global Footer Policy
- VPN Console

Importing profile group and RADIUS dynamic start server

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

Push update in bi-directional static NAT

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

Configure the following settings on FortiManager:

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

Upgrade Information

Upgrading to FortiManager 5.2.6

For information about upgrading your FortiManager device to 5.2.6, see *FortiManager 5.2.6 Upgrade Guide*.

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
execute format {disk | disk-ext4}
```

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bits firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bits package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bits package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

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

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://wwwfortinet.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 5.2.6 support

The following table lists 5.2.6 product integration and support information:

Web Browsers	• Microsoft Internet Explorer™ 11.0 • Mozilla Firefox version 45 • Google Chrome version 49 Other web browsers may function correctly, but are not supported by Fortinet. Please make sure your computer's screen resolution is set to at least 1280x1024. Otherwise, web pages may not be displayed properly.
FortiOS/FortiOS Carrier	FortiManager 5.2.6 expects to support the following versions: • 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 Compatibility with FortiOS Versions on page 26. • 5.2.2 to 5.2.6 • 5.2.1 FortiManager 5.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 26. • 5.2.0 FortiManager 5.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility with FortiOS Versions on page 26. • 5.0.4 to 5.0.13 FortiManager 5.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.13, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 26. • 4.3.2 to 4.3.18 For the latest information, see FortiOS and FortiManager Compatibility at http://docs.fortinet.com/d/fortimanager-compatibility

FortiAnalyzer	• 5.2.0 and later • 5.0.0 and later • 5.0.0 to 5.0.10
FortiCache	• 3.0.0 to 3.0.8
FortiClient	• 5.2.0 and later • 5.0.4 and later
FortiMail	• 5.2.7 • 5.1.5 • 5.0.8
FortiSandbox	• 2.1.2 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 6.2 • Linux KVM Redhat 6.5 • Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2 • OpenSource XenServer 4.2.5 **VMware** • ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0

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

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

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

Feature support

The following table lists FortiManager feature support for managed platforms.

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

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓	✓	
Chinese (Traditional)	✓	✓	
French		✓	
Japanese	✓	✓	
Korean	✓	✓	

Language	GUI	Reports	Documentation
Portuguese		✓	
Spanish		✓	

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
<password> <file name>
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
<password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
<password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiManager CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 5.2.6.

Supported FortiGate models

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-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-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC,FG-3810D-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FCT-5902D, FS-5203B	5.2

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FGT-3000D **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-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FG-70D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5903C, FCT-5913	5.0

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30B, FG-40C, FG-50B, FG-51B, FG-60B, FG-60C, FG-60C-POE, FG-60C-SFP, FG-80C, FG-80CM, FG-82C, FG-100A, FG-100D, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-311B, FG-400A, FG-500A, FG-600C, FG-620B, FG-621B, FG-800, FG-800C, FG-800F, FG-1000A, FG-1000AFA2, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001, FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001FA2, FG-5001FA2-LENC, FG-5002A, FG-5002A-LENC, FG-5002FB2, FG-5005FA2, FG-5005FA2-2G, FG-5005FA2-4G, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-600C-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-50B-LENC, FG-51B-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-1000A-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30B, FWF-40C, FWF-50B, FWF-60B, FWF-60C, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM **FortiGate Rugged:** FGR-100C **FortiGate One:** FG-ONE **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-XEN, FG-VMX **FortiSwitch:** FS-5203B	4.3

Supported FortiCarrier models

Model	Firmware Version
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.2

Model	Firmware Version
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.0
FortiCarrier: FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2, FCR-60B, FCR-60C **FortiCarrier DC:** FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC	4.3

Supported FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-HV	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV	5.0

Supported FortiMail models

Model	Firmware Version
FortiMail: FE-200D, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2

Model	Firmware Version
FortiMail: FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1
FortiMail: FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0

Supported FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0 1.4
FortiSandbox: FSA-1000D, FSA-3000D	1.3 1.2

Supported FortiSwitch ATCA models

Model	Firmware Version
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3 4.2

Supported FortiWeb models

Model	Firmware Version
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64	5.3
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64	5.2 5.1 5.0

Supported FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D **FortiCache VM:** FCH-VM64	3.0 and later

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.2.6.

Compatibility issues with FortiOS 5.2.7

The following table lists interoperability issues that have been identified with FortiManager version 5.2.6 and FortiOS version 5.2.7.

Bug ID	Description
365782	Install may fail on system global optimize or system fips-cc entropy-token.
365766	Retrieve may fail when there are more than 50 portals within a VDOM.
365757	Retrieve may fail on LDAP User Group if object filter has more than 511 characters.

Compatibility issues with FortiOS 5.2.3

The following table lists interoperability issues that have been identified with FortiManager version 5.2.6 and FortiOS version 5.2.3.

Bug ID	Description
289068	FortiManager may report a failure on the radio-2 setting with 802.11ac when installing a new VDOM. Workaround: Please run a `Retrieve` after the install.

Compatibility issues with FortiOS 5.2.2

The following table lists interoperability issues that have been identified with FortiManager version 5.2.6 and FortiOS version 5.2.2.

Bug ID	Description
287632	Install fails with the default SSL VPN self-sign certificate.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.2.6 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 5.2.6 and FortiOS version 5.2.0.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Compatibility issues with FortiOS 5.0.5

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.1 and FortiOS version 5.0.5.

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Compatibility issues with FortiOS 5.0.4

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.6 and FortiOS version 5.0.4.

Bug ID	Description
226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
226078	When the password length is increased to 128 characters, the installation fails.
226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.
226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS 5.0.5.
226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Resolved Issues

The following issues have been fixed in 5.2.6. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
363554	Policy import may fail due to GTP profile address group.
355528	When users remove a FortiGate with a FortiExtender attached, the FortiExtender device is not removed.
306284	FortiManager installs virtual-switch and system interface in a wrong order.
306235	FortiManager may not show available interfaces for hardware switch.
305734	List of available folders should be sorted in alphabetical order during the import policy process.
305187	FortiManager shows the same installed policy package name for two different VDOMs.
305044	The maximum number of VLANs per interface for FGT-30D is incorrect.
301576	Some CLI-only objects have pre-selected values and these values cannot be removed.
300756	Creating/deleting an IP MAC binding in a DHCP server results in “Web Server Error 500”.
299947	Configuring the prefix value in the router prefix list on a 64-bit platform returns “runtime error 23: beyond the boundary".
299584	Users cannot configure alert email for FortiOS from Device Manager.
297897	Interface associations may be lost for address objects when a VDOM has dynamic mappings overriding the originally imported global objects.
297888	The output for CLI “diagnose dvm device list” shows incorrect policy package status for VDOMs in different ADOMs of a FortiGate.
296946	Import operation identifies constant conflicts between the UNSET and EMPTY values for various objects .

Bug ID	Description
296595	Editing the ha-mgmt interface under Device Manager triggers Web Server Error 500.
295908	Under the Device Manager of FortiManager, the FortiGuard License of FortiGate is shown as *Unknown*.
295861	Users cannot configure multiple DNS servers on the interface editing page.
295775	Installation of ospf md5-key into FGT 4.3 in ADOM v4.3 fails.
295606	Invalid IP range is defined on FortiManager for a dial-up IPSec VPN.
295596	After an upgrade from 5.0.11, FortiManager shows an empty interface list and a blank HA configuration page for FortiGate.
294715	The value range of Tx Power is inconsistent between FortiManager and FortiGate.
292218	When creating DHCP relay, error “runtime error 89: duplicate ip in the list” may show up.
290999	Users cannot configure the DHCP Relay on Hardware Switch interface when it is set to *Internal*.
288495	Users cannot delete device VDOM via Device Manager menu “Virtual Domain”.
281328	HA-Reserved management interface is displayed under all ADOMs within the same FortiGate.

Policy and Objects

Bug ID	Description
363970	Users may not be able to open the results of Policy Consistency Check.
357099	FortiManager does not allow users to configure an IPSec policy with a zone object in the Outgoing Interface.
355672	FortiManager should allow overlapping a VIP that has "src-filter" set and with "any" in the same policy.
306434	The “Where used” function may show the dynamic mapping of an address that has already been deleted.
305726	FortiManager cannot install guest user group authtimeout to FortiGate.

Bug ID	Description
302913	Changes of the order of objects under identity-based-policy will not be installed on FortiGate.
301695	Field Service and Schedule are ignored during policy consistency check.
301247	Setting a Virtual IP as the destination in a policy does not work when the External Interface binding of the Virtual IP is different form the destination interface in the policy.
300814	When there are a large number of firewall policies, it may take a long time to clone/edit a policy.
300370	If the user's local time is different from FortiManager system time, editing a one-time schedule may change its content.
299515	FortiManager does not report an error when users add an SSL-VPN interface to a zone.
299494	GUI may get stuck after OK button is double-clicked on the object edit page.
298774	Policy package status does not change when a global policy is deleted.
296766	Installation will fail when an interface of a policy is changed to the management interface.
295944	Installation of a policy package changes the UUID of identity policies.
295828	Multiple users cannot generate preview at the same time.
295827	When there are a large number of packages and policies, the "where used" function may stop working.
295745	When installing a v5.0 Policy Package to a v5.2 FortiGate device, firewall rules are not installed in the correct order.
295557	Changes to User Group that reference an IPSec Phase1 object are not installed.
295540	FortiManager should not install "report layout – purge" with every policy package installation.
294162	Changing the fwpolicy-implicit-log settings at device level does not change the Policy Package status.
293949	FortiManager cannot manage all SIP settings in a VOIP profile.
293941	Making changes in the SSL-VPN portal my not trigger changes in policy package status.

Bug ID	Description
293431	Canceling a Policy Package installation preview may result in changes in Device level cached DB.
293392	Some fields within ADOM may be vulnerable to XSS attacks.
291625	The ha-mgmt-interface can be added as an interface in “local-in-policy”.
291163	A warning message is not always displayed when adding a duplicate address object.
288655	The Policy interface selection drop-down list may not show zones or interfaces.
276973	FortiManager should not allow users to delete a policy package folder when it is the last item within the policy package menu.
276806	Scheduled installations from a TACAS+ wildcard user do not work as expected.

Revision History

Bug ID	Description
295338	ADOM revision may not be able to revert to a previous version after any type of changes.
283961	Changing the firewall address type from FQDN to IP results in installation failure.

Script

Bug ID	Description
301394	No error is returned when function createScript misses parameter “target”.
235769	The append command is not supported by FortiManager.

Services

Bug ID	Description
355161	Downstream FortiManager may not be able to get account IDs for licenses.

Bug ID	Description
310097	Users may not be able to access FortiManager when many FortiGate units request updates.
310069	The random setting of AV/IPS update-schedule time does not work.
298651	When receiving auto-updates from a large number of FortiGates, FortiManager may run out of memory.
294076	When there are many requests, FortiManager VM users may not be able to log in.
287811	The um_db_service process may consume high IO resource.

System Settings

Bug ID	Description
355150	FortiManager HA is out of synchronization when moving the CLI console widget on the Dashboard page.
308892	LDAP user search on FortiManager is always “cn” based.
303922	Users cannot select individual TSL versions.
296028	When RADIUS authentication is configured with wildcard authentication, some actions are not logged with the correct user name.
289207	After a configuration change on FortiGate, FortiManager may falsely report that certificate private keys have changed.
278873	False high memory SNMP traps are sent when memory utilization is lower than trap-low-memory-threshold.

VPN Console

Bug ID	Description
307433	FortiManager converts a /32 subnet into an IP address when configuring IPSec phase 2 settings.
301375	Adding or deleting a Spoke in a Star topology VPN changes the policy package status of existing Spokes.

Others

Bug ID	Description
303117	After removing the secondary FortiManager from a FortiManager cluster, FortiGate does not remove the serial number of the secondary FortiManager from its configuration.
302389	Addressed the CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, and CVE-2015-3196 vulnerabilities.
294879	Within a HA cluster, the password for the admin account is not synchronized to that for the slave when password policy is enabled and triggered.
294410	Users may not be able to restore a backup due to invalid “fmupdate server-access-priorities” configuration.
294191	When users use JSON API to install policy followed by an immediate unlock request, the installation may fail.
293111	If users change the Management Interface settings from GUI, fclupdates in serviceaccess of the interface will be removed.
280054	"Diagnose dvm check-integrity" reports "Checking duplicate device vdoms" errors without fixing them automatically.

Common Vulnerabilities and Exposures

Bug ID	Description
356873	FortiManager 5.2.6 is no longer vulnerable to the following CVE-References: • 2016-0702 • 2016-0703 • 2016-0704 • 2016-0705 • 2016-0797 • 2016-0798 • 2016-0799 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.2.6. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Management

Bug ID	Description
364366	Unauthorized APs may not be shown on FortiManager.

Device Manager

Bug ID	Description
294021	SSL-VPN may not list all the available portals when some portals have been mapped by other FortiGate devices or VDOMs. Workaround: Use CLI to copy the missing portals from ADOMs to the database of the targeted FortiGate device.

Revision History

Bug ID	Description
365412	Due to memory leaks, FortiManager may not be able to install to many devices or install a large policy package.
305369	Install device changes may fail on the dh-params and upload-option settings. Workaround: Run a retrieve on the affected devices.

Services

Bug ID	Description
365743	FortiManager may not be able to provide update services to FortiGate HA cluster.
364406	FortiGuard server may run out of memory and crash.

System Settings

273966	Users cannot change an administrator's password with Internet Explorer 11.

FortiGuard Distribution Servers (FDS)

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

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

FortiGuard Center update support

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

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	• 5.0.0 and later • 5.2.0 and later	✔		✔	
FortiClient (Windows)	• 4.3.0 and later	✔			
FortiClient (Windows)	• 4.2.0 and later	✔	✔		✔
FortiClient (Mac OS X)	• 5.0.1 and later • 5.2.0 and later	✔		✔	
FortiMail	• 4.2.0 and later • 4.3.0 and later • 5.0.0 and later • 5.1.0 and later • 5.2.0 and later	✔	✔		
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later	✔			
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
```