FortiManager Release Notes

VERSION 5.2.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 2, 2015

FortiManager 5.2.1 Release Notes

02-521-261104-20150602

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Supported models 6
What's new in FortiManager 5.2.1 6
Special Notices **7**
SQL database rebuild 7
ADOM upgrade 7
Web Portal support 7
CLI commands for configuring dynamic objects 7
FortiManager VM 8
FortiAnalyzer feature set 8
FortiGate firmware upgrade 9
System time on FortiManager VM 9
Memory requirement for FortiManager VM64-HV 9
ADOM for FortiCarrier 9
FortiOS 5.0 override server setting for FortiGuard Services 9
Example 1: Antivirus/IPS 10
Example 2: Web filtering/Antispam 10
Update services provided to FortiMail 4.2 devices 11
Endpoint management 11
FortiManager VM license check 11
Multi-language display support 11
Importing a FortiManager generated policy 12
Importing profile group and RADIUS dynamic start server 12
Push update in bi-directional static NAT 12
FortiOS 5.2.3 Support 12
Upgrade Information **13**
Upgrading from FortiManager 5.2.0 13
Upgrading from FortiManager 5.0.6 or later 13
Downgrading to previous firmware versions 13
FortiManager VM firmware 13
Firmware image checksums 14
SNMP MIB files 14
Product Integration and Support **15**

FortiManager 5.2.1 support 15
Feature support 16
Language support 17
Supported models 18
Compatibility with FortiOS Versions 25
Compatibility issues with FortiOS 5.2.3 25
Compatibility issues with FortiOS 5.2.1 25
Compatibility issues with FortiOS 5.2.0 25
Compatibility issues with FortiOS 5.0.10 26
Compatibility issues with FortiOS 5.0.5 26
Compatibility issues with FortiOS 5.0.4 26
Resolved Issues 28
Device Manager 28
FortiOS Carrier 29
Other 29
Policy and Objects 30
Revision History 30
Script 31
Services 31
System Settings 31
VPN Console 32
Known Issues 33
Device Manager 33
Policy and Objects 33
Services 33
System Settings 34
Upgrade 34
FortiGuard Distribution Servers (FDS) 35
FortiGuard Center update support 35

Change Log

Date	Change Description
2014-12-12	Initial release.
2014-12-15	Updated the Compatibility with FortiOS Versions chapter.
2014-12-18	Minor document update.
2015-03-24	Added FortiOS support and compatibility details.
2015-04-10	Updated the Upgrade chapter.
2015-04-14	Updated build number.
2015-04-30	Added VM Partition and Firmware information to the Upgrade Information chapter.
2015-05-22	Minor update to Special Notices > FortiOS 5.2.3 Support and Compatibility with FortiOS Versions > Compatibility issues with FortiOS 5.2.3.
2015-06-02	Updated Upgrade Information Chapter.

Introduction

This document provides the following information for FortiManager 5.2.1 build 0662:

- Supported models
- What's new in FortiManager 5.2.1
- Special Notices
- Upgrade Information
- Product Integration and Support
- Compatibility with FortiOS Versions
- Resolved Issues
- Known Issues
- FortiGuard Distribution Servers (FDS)

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

Supported models

FortiManager version 5.2.1 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM32, FMG-VM64, and FMG-VM64-HV.

What's new in FortiManager 5.2.1

The following is a list of new features and enhancements in 5.2.1.

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

- Toolbar buttons for the Policy section.
- Install for admin with Restricted profile.
- Approval matrix for Workflow.
- IPv6 support for FG-FM connections.
- Unify JSON APIs with XML APIs.
- Added version to JSON APIs for Policy Package & Objects.
- Optional dynamic VIP default values.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.2.1.

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.

ADOM upgrade

Upgrade is available for ADOM version 4.3 to migrate to version 5.0.

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 5.2.1, 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 and 4.3 devices only. FortiOS version 5.2 has a different behavior.

Ports used by FortiGuard services

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

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

Example 1: Antivirus/IPS

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

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

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

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

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

Example 2: Web filtering/Antispam

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

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

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

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

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

Update services provided to FortiMail 4.2 devices

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

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

Endpoint management

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

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

FortiManager VM license check

As 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
```

FortiOS 5.2.3 Support

FortiGate units running FortiOS 5.2.3 managed by FortiManager 5.2.1 may report installation failures on newly created VDOMs or after a factory reset of the FortiGate Unit even after a retrieve and re-import policy. The issue will be addressed in FortiManager 5.2.2 and later releases.

Upgrade Information

Upgrading from FortiManager 5.2.0

FortiManager 5.2.1 supports upgrade from 5.2.0.

Upgrading from FortiManager 5.0.6 or later

FortiManager version 5.0.7 or later has re-sized the flash partition storing system firmware. If your FortiManager is running 5.0.6, you will need to change the hard disk provisioned size to more than 512 MB in your VM environment before powering on the FortiManager VM. The secondary firmware and System Settings stored in the partition is lost after upgrade. Please reconfigure System Settings as needed.

For information on upgrading your FortiManager device, see the *FortiManager 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 Web-based Manager 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 Microsoft Hyper-V Server and VMWare ESX/ESXi virtualization environments.

Microsoft Hyper-V Server

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

VMware ESX/ESXi

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

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/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 5.2.1 support

The following table lists 5.2.1 product integration and support information:

Web Browsers	• Microsoft Internet Explorer versions 10 and 11 • Mozilla Firefox version 33 • Google Chrome version 38 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 5.2.3 • 5.2.2 • 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 Compatibility with FortiOS Versions. • 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 Compatibility with FortiOS Versions. • 5.0.4 to 5.0.10 FortiManager 5.2.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.04 to 5.0.10, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions. • 4.3.2 to 4.3.18
FortiAnalyzer	• 5.2.0 and 5.2.1 • 5.0.0 to 5.0.9
FortiCache	• 3.0.0 and later
FortiClient	• 5.2.0 and later • 5.0.4 and later
FortiMail	• 5.2.2 • 5.1.4 • 5.0.7

FortiSandbox	• 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	• 5.3.3 • 5.2.4 • 5.1.4 • v5.0.6
Syslog	• Standard Syslog
Virtualization	• Microsoft Hyper-V 2008 R2 and 2012 **VMware** • ESX version 4.0 and 4.1 • ESXi version 4.0, 4.1, 5.0, 5.1, and 5.5

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

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

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

Feature support

The following table lists FortiManager feature support for managed platforms.

Feature support per platform

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✔	✔	✔	✔

Feature support per platform

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

Language support

The following table lists FortiManager language support information.

Language support

Language	Web-based Manager	Reports	Documentation
English	✔	✔	✔
Chinese (Simplified)	✔	✔	
Chinese (Traditional)	✔	✔	
French		✔	
Hebrew		✔	
Hungarian		✔	
Japanese	✔	✔	
Korean	✔	✔	
Portuguese		✔	
Russian		✔	
Spanish		✔	

To change the FortiAnalyzer 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 5.2.1.

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-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-94D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700DX, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-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-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 **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.2

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-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-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-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-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-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.0

Supported FortiGate models

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-1000, 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-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 **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-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
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 **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-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-HV	5.2

Supported FortiAnalyzer models

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

Supported FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

Supported FortiSwitch ATCA models

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

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-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64	5.3.3
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64	5.2.4 5.1.4 5.0.6

Supported FortiCache models

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

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.2.1.

Compatibility issues with FortiOS 5.2.3

Compatibility issues with FortiOS 5.2.3

Bug ID	Description
271059	FortiGate units running FortiOS 5.2.3 managed by FortiManager 5.2.1 may report installation failures on newly created VDOMs or after a factory reset of the FortiGate Unit even after a retrieve and re-import policy.The issue will be addressed in FortiManager 5.2.2 and later releases.

Compatibility issues with FortiOS 5.2.1

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

Compatibility issues with FortiOS 5.2.1

Bug ID	Description
0262584	When creating a VDOM for the first time it fails.
0263896	`config retrieve` fails if using the Fortinet_CA_SSLProxy or Fortinet_SSLProxy certificate.

Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.1 and FortiOS version 5.2.0.

Compatibility issues with FortiOS 5.2.0

Bug ID	Description
0262348	Install may fail for `config endpoint-control profile` and `set forticlient-ef-profile default`.
0262584	When creating a VDOM for the first time it fails.

Compatibility issues with FortiOS 5.2.0

Bug ID	Description
0263896	`config retrieve` fails if using the Fortinet_CA_SSLProxy or Fortinet_SSLProxy certificate.
0263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Compatibility issues with FortiOS 5.0.10

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.1 and FortiOS version 5.0.10.

Compatibility issues with FortiOS 5.0.10

Bug ID	Description
0263526	Install fails for service `protocol-number`.

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.

Compatibility issues FortiOS 5.0.5

Bug ID	Description
0230199	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 5.2.1 and FortiOS version 5.0.4.

Compatibility issues with FortiOS 5.0.4

Bug ID	Description
0226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.

Compatibility issues with FortiOS 5.0.4

Bug ID	Description
0226078	When the password length is increased to 128 characters, the installation fails.
0226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
0226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.
0226203	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.
0226236	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.
0230199	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 5.2.1. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Resolved device manager issues

Bug ID	Description
0209043	Opening a second terminal CLI session may connect to the wrong device.
0220537	Device Manager does not display an error when configuring a device with a duplicated name to an existing device within the same ADOM.
0229635	FortiManager prompts an error when modifying the soft switch with only one interface.
0229738	FortiManager cannot create two dead gateway detection profiles on the same interface.
0241871	There are some inconsistencies in the VDOM level log settings.
0242085	FortiManager cannot bring up or down multiple tunnels at once within a Central VPN Console ADOM.
0248536	Import Wizard imports all duplicated firewall addresses as dynamic objects instead of duplicated objects.
0249200	FortiManager cannot change the IPsec phase1 remote gateway's IP address.
0251349	After upgrading an ADOM to version 5.0, SCTP anomalies are missing from DoS policies.
0252558	FortiManager is unable to display Central VPN query data.
0253900	When FortiManager is upgraded to version 5.2 and FortiGate has an address group defined in IPsec phase 2, FortiManager deletes the phase 2 interface.
0254243	Hardware contract details are not correctly reported on FortiManager.
0254260	When adding an IPsec phase1 proposal, FortiManager automatically adds DES-MD5 even though it is not selected.
0254905	FortiManager prompts a data error when importing a policy package and there are more than 700 interfaces within a VDOM.
0257853	After a cluster failover, FortiManager tries to push the same `mgmt1` IP address and `elbc-base-ctl` IP address to all the slave blades.

FortiOS Carrier

Resolved FortiOS Carrier issues

Bug ID	Description
0251685	The GTP profiles column is not available on the Policy Package page.
0252603	FortiManager Web-based Manager does not accept GTP profile and APN names containing a period character.

Other

Other resolved issues

Bug ID	Description
0251003	FortiManager cannot run a Policy Package Installation Preview via JSON APIs.
0251307	The *comments* field cannot be filled when adding a VDOM to a device via the JSON API.
0251709	The browser tab closes after installing or importing a policy package.
0252377	Email Diff does not work for Policy Packages in folder.
0252889	The `diagnose dvm adom list` CLI command does not indicate the mode and VPN management.
0254112	The `admintimeout` setting should be removed since it is duplicated with `idle_timeout`.
0255356	There is an XSS vulnerability in Device Manager's Revision History page.
0255569	CVE-2014-6271: Weakness for remote exploit.
0256997	CVE-2010-5107: OpenSSH slot exhaustion DoS.

0257316	CVE-2014-3566: SSLv3 POODLE vulnerability. A CLI command to control the SSL protocol has been added:
	`config system global`
	`set ssl-protocol {tlsv1 | sslv3}`

0257778	Upgraded OpenSSL for the following vulnerabilities: • CVE-2014-3513: DTLS SRTP memory leak • CVE-2014-3567: Session ticket memory leak • CVE-2014-3568: Build option no-ssl3 is incomplete • SSL 3.0 Fallback protection

Policy and Objects

Resolved policy and objects issues

Bug ID	Description
0244396	FortiManager cannot search objects with the keyword `Dynamic`.
0245267	The *Where used* feature does not work for a predefined firewall service in a version 4.3 ADOM.
0248409	Web Filter Exempted Category feature disappears from settings.
0248805	Destination address setting for web-proxy identity based policy does not work as expected.
0250443	Install and verification failures are prompted on `system replacemsg auth` setting after FortiManager is upgraded.
0250580	FortiManager prompts an error when deleting UDP/SCTP protocol data related to custom services.
0251156	Per-User BWL feature is not visible on FortiManager.
0252030	Renaming a firewall address object no longer displays in its associated policy.
0254540	FortiManager prompts an error when creating an IP Pool with a fixed port range.
0255300	FortiManager should not add the option `mailbomb unhandled` when creating an AV profile.
0255700	The `exec fsso refresh` CLI command causes a change on FortiGate status to `Warning`.
0256654	FortiManager allows administrators to create a policy that is invalid on FortiGate.
0257721	FortiManager is unable to add more than one SSL VPN bookmark for HTTP/HTTPS in single group.
0258695	User Group entries in the Web Filter Profile are lost when editing the Authenticate list.
0258961	FortiManager is unable to create SSL/SSH Inspection Profiles when an ADOM is locked.

Revision History

Resolved revision history issues

Bug ID	Description
0224133	Install fails when changing an identity based policy to a web-proxy policy.
0228964	FortiManager should include the device name when downloading a revision file.

Resolved revision history issues

Bug ID	Description
0252318	ADOM revision storage limitation should be enforced.
0252383	FortiManager is missing the blue vertical bar for the Profiles column & No Authentication column in the Diff report.
0253605	Installation fails if there is a space character in FortiGate's VLAN name.
0255392	Auto-install with Global policy assign hangs when there is a large number of devices.

Script

Resolved script issues

Bug ID	Description
0215376	FortiManager cannot change the target of a script to Run on FortiGate Directly (Via CLI).
0252400	Incorrect and inconsistent Dynamic Local Certificate objects can be created via a CLI script.
0257679	FortiManager cannot set VDOM partitioning on a FortiGate Virtual Cluster.

Services

Resolved services issues

Bug ID	Description
0249082	Service Status does not reflect the GeoIP version.
0253070	FortiManager fails to push IRDB and Botnet database to FortiGate with the message *upd_install_pkg-IRDB is unauthorized*.

System Settings

Resolved system settings issues

Bug ID	Description
0235920	FortiManager is unable to use the CLI Java console. The following error is displayed: `Too many concurrent connections.`
0237798	FortiManager should support IPv6 NTP server peer.

Resolved system settings issues

Bug ID	Description
0247274	FortiManager cannot use SSH with remote command if the admin account contains a password.
0251713	FortiManager should avoid logging unnecessary SQL errors to the event log when deleting a Policy Package.
0252193	FortiManager should generate an Event log when upgrading an ADOM.
0252198	FortiManager is unable to view all ADOMs from System Settings.
0252456	The space character should be allowed in an SNMP Community name.
0252624	FortiManager is unable to upgrade a version 4.3 Central VPN Console ADOM to version 5.0.
0257217	Event logs should not record Install Preview as an install.

VPN Console

Resolved VPN console issues

Bug ID	Description
0255212	The external gateway role *Spoke* is changed to *Hub* if node settings are changed.
0257536	VPN Console does not recognize an egress interface configured as DHCP using DDNS.

Known Issues

The following issues have been identified in 5.2.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Known device manager issues

Bug ID	Description
0259988	FortiManager may not be able to set guaranteed resources in VDOM properties.
0262163	FortiGate's configuration status is shown as *out-of-sync* after installing a policy package and configuration setting at the same time.

Policy and Objects

Known policy and objects issues

Bug ID	Description
0259333	Administrators are unable to change or remove SMS configuration under user definition.
0259512	Local categories are always imported with a disable status.
0259985	Application sensor clone action does not work correctly.
0260177	When editing an IPS sensor, signatures from extended IPS database are not available.
0261689	FortiManager may not be able to delete VIP objects although they are not in use.
0261982	Indication that a column filter is active should not disappear after a column is moved.
0262208	*Where Used* may not work in some cases.

Services

Known services issues

Bug ID	Description
0260650	When FortiManager is in closed network mode, support contract information should be displayed when FortiManager is using the proper entitlement file.

System Settings

Known system settings issues

Bug ID	Description
0260489	After upgrading a version 4.3 ADOM to version 5.0, all mapped IP addresses are removed on all VIPs.

Upgrade

Known upgrade issues

Bug ID	Description
0264051	Installing a version 5.0 ADOM policy package to a version 5.2 FortiGate will delete all policies and re-add them. There may also be missing policies.

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:

FortiGuard Center update support

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
```