FortiManager v5.2.0
Release Notes

FortiManager v5.2.0 Release Notes

June 02, 2015

02-520-249292-20150602

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-08-25	Initial release.
2014-09-03	Added a special notice for Web Portal support.
2014-09-05	Added 0252558 to the Known Issues chapter.
2014-09-08	Updated the Compatibility with FortiOS Versions chapter.
2014-09-09	Corrected FortiCache support information.
2014-09-23	Added FortiOS/FortiOS Carrier v5.2.1 support. Updated the Compatibility with FortiOS Versions chapter.
2014-09-25	Removed FSA-VM from Supported FortiSandbox models.
2014-11-13	Updated upgrade information.
2015-05-01	Updated the VM Partition Information in the Upgrade Information chapter.
2015-06-02	Updated Upgrade Information chapter.

Introduction

This document provides the following information for FortiManager v5.2.0 build 0618:

- Supported models
- What's new in FortiManager v5.2.0
- Special Notices
- Upgrade Information
- Product Integration and Support
- Compatibility with FortiOS Versions
- Resolved Issues
- Known Issues
- FortiGuard

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

Supported models

FortiManager v5.2.0 supports the following models:

Table 1: Supported models

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

What's new in FortiManager v5.2.0

The following is a list of new features and enhancements in v5.2.0

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

- Device Manager Web-based Manager improvements
- Policy table usability improvements
- Workflow mode
- Restricted Admin profile
- CLI-Only Objects menu in Device Manager and Policy & Objects
- Dynamic object tables at the ADOM level
- Improved model device wizard
- Central AP management filtering
- Improved logging of script execution
- Firmware version displayed is consistent with FortiOS v5.2
- VPN Monitor status pages in Device Manager
- Support for VRRP group ID and VRRP status from FortiGate
- Policy and object improvements – Object Grouping
- UUID support
- Two-factor authentication for administration log on
- FortiExtender support
- Run Tcl script to access local databases
- Dynamic address group
- Flexible FDS override list management
- FIPS-CC compliance for FortiManager
- Update service to FortiWeb (Antivirus only)
- Improved Web-based Manager consistency
- WF/AS communication to FortiManager via TCP port 80/443

Special Notices

This section highlights some of the operational changes that administrators should be aware of in v5.2.0.

ADOM upgrade

Upgrade is available for ADOM version 4.3 to migrate to version 5.0. Currently, there is no ADOM upgrade option for ADOM version 5.0 to move to version 5.2.

Web Portal support

Web Portal is no longer available as it has been replaced by Restricted Admin Profile in v5.2. Users can still access web portal content via the Web Portal API services.

CLI commands for configuring dynamic objects

In v5.2, 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 v5.2.0 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 FortiManager will reboot with the FortiAnalyzer features enabled.

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

In v5.2.0, 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 v5.0 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 v5.0 and v4.3 devices only. FortiOS v5.2 has a different behavior.

Table 2 lists the ports used by FortiGuard Services.

Table 2: FortiGuard services ports

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 v4.2 devices

Please enable the following option in order to provide update services to FortiMail v4.2 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 v5.0.0 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 v5.2.0 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 from FortiManager v5.0.6 or later

FortiManager v5.2.0 supports upgrade from v5.0.6 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.

Upgrading from FortiManager v5.0.5 or earlier

In order to accommodate the re-sizing of the flash partition, you MUST upgrade to v5.0.6 first.

For information on upgrading your 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 both VMware ESX/ESXi and Microsoft Hyper-V Server 2008 R2/2012 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 FortiManager VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiManager 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 v5.00 file folder.

Product Integration and Support

FortiManager v5.2.0 support

The following table lists v5.2.0 product integration and support information.

Table 3: FortiManager v5.2.0 support

Web Browsers	• Google Chrome version 36 • Microsoft Internet Explorer versions 10 and 11 • Mozilla Firefox versions 30 and 31 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• v5.2.1 FortiManager v5.2.0 is fully tested as compatible with FortiOS/FortiOS Carrier v5.2.1, with some minor interoperability issues. For information, see "Compatibility with FortiOS Versions" on page 22. • v5.2.0 FortiManager v5.2.0 is fully tested as compatible with FortiOS/FortiOS Carrier v5.2.0, with some minor interoperability issues. For information, see "Compatibility with FortiOS Versions" on page 22. • v5.0.4 to v5.0.9 FortiManager v5.2.0 is fully tested as compatible with FortiOS/FortiOS Carrier v5.04 to v5.0.9, with some minor interoperability issues. For information, see "Compatibility with FortiOS Versions" on page 22. • v4.3.2 to 4.3.18
FortiAnalyzer	• v5.2.0 • v5.0.0 and later
FortiMail	• v5.1.3 • v5.0.6
FortiWeb	• v5.2.0 • v5.1.4 • v5.0.6
FortiCache	• v3.0.0
FortiSwitch ATCA	• v5.0.0 and later • v4.3.0 and later • v4.2.0 and later

Table 3: FortiManager v5.2.0 support (continued)

FortiClient	• v5.2.0 and later • v5.0.4 and later
FortiSandbox	• v1.4.0 and later • v1.3.0 • v1.2.0 and v1.2.3
Virtualization Software	• Microsoft Hyper-V Server 2008 R2 and 2012 • VMware ESX versions 4.0 and 4.1 • VMware ESXi versions 4.0, 4.1, 5.0, 5.1, and 5.5

Feature support

The following table lists FortiManager feature support for managed platforms.

Table 4: Feature support per platform

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

Language support

The following table lists FortiManager language support information.

Table 5: Language support

Language	Web-based Manager	Reports	Documentation
English	✔	✔	✔
Chinese (Simplified)	✔	✔	
Chinese (Traditional)	✔	✔	

Table 5: Language support (continued)

Language	Web-based Manager	Reports	Documentation
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 v5.2.0.

Table 6: Supported FortiGate models

Model	Firmware Version
FG-20C, FG-20C-LENC, FWF-20C, FG-20C-ADSL-A, FWF-20C-ADSL-A, FG-30D, FWF-30D, FG-30D-POE, FWF-30D-POE, FG-40C, FG-40C-LENC, FWF-40C, FG-60C, FG-60C-LENC, FWF-60C, FG-60C-POE, FG-60C-SFP, FWF-60CM, FWF-60CX-ADSL-A, FG-60D, FWF-60D, FG-60D-POE, FWF-60D-POE, FG-80C, FG-80C-LENC, FG-80C-DC, FG-80CM, FWF-80CM, FWF-81CM, FG-90D, FWF-90D, FG-90D-POE, FWF-90D-POE, FG-100D, FG-100D-LENC, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-LENC, FG-200B-POE, FG-200D, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300C-LENC, FG-300C-DC, FG-310B, FG-310B-DC, FG-310B-LENC, FG-311B, FG-600C, FG-600C-DC, FG-600C-LENC, FG-620B, FG-620B-DC, FG-621B, FG-621B-DC, FG-800C, FG-800C-DC, FG-1000C, FG-1000C-DC, FG-1000C-LENC, FG-1240B, FG-1240B-DC, FG-1240B-LENC, FG-3016B, FG-3040B, FG-3040B-DC, FG-3040B-LENC, FG-3140B, FG-3140B-DC, FG-3140B-LENC, FG-3240C, FG-3240C-DC, FG-3600C, FG-3600C-DC, FG-3810A, FG-3810A-DC, FG-3810A-LENC, FG-3950B, FG-3950B-DC, FG-3950B-LENC, FG-3951B, FG-3951B-DC, FG-5001A, FG-5001B, FG-5001C, FG-5101C FGR-60D FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN FS-5203B	v5.2
FG-20C, FG-20C-LENC, FWF-20C, FG-20C-ADSL-A, FWF-20C-ADSL-A, FG-30D, FWF-30D, FG-30D-POE, FWF-30D-POE, FG-40C, FG-40C-LENC, FWF-40C, FG-60C, FG-60C-LENC, FWF-60C, FG-60C-POE, FG-60C-SFP, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FG-60D, FWF-60D, FG-60D-3G4G-VZW, FG-60D-POE, FWF-60D-POE, FG-70D, FG-80C, FG-80C-LENC, FG-80C-DC, FG-80CM, FWF-80CM, FWF-81CM, FG-80D, FG-90D, FWF-90D, FG-90D-POE, FWF-90D-POE, FG-92D, FG-94D-POE, FG-100D, FG-100D-LENC, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-LENC, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300C-LENC, FG-300C-DC, FG-300D, FG-310B, FG-310B-DC, FG-310B-LENC, FG-311B, FG-500D, FG-600C, FG-600C-DC, FG-600C-LENC, FG-620B, FG-620B-DC, FG-621B, FG-621B-DC, FG-800C, FG-800C-DC, FG-1000C, FG-1000C-DC, FG-1000C-LENC, FG-1240B, FG-1240B-DC, FG-1240B-LENC, FG-1500D, FG-3016B, FG-3040B, FG-3040B-DC, FG-3040B-LENC, FG-3140B, FG-3140B-DC, FG-3140B-LENC, FG-3240C, FG-3240C-DC, FG-3600C, FG-3600C-DC, FG-3700D, FG-3810A, FG-3810A-DC, FG-3810A-LENC, FG-3950B, FG-3950B-DC, FG-3950B-LENC, FG-3951B, FG-3951B-DC, FG-5001A, FG-5001B, FG-5001C, FG-5001D, FG-5101C FGR-60D, FGR-100C FGV-70D4 FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN FS-5203B	v5.0

Table 6: Supported FortiGate models (continued)

Model	Firmware Version
FG-20C, FG-20C-LENC, FWF-20C, FG-20C-ADSL-A, FWF-20C-ADSL-A, FG-30B, FWF-30B, FG-40C, FG-40C-LENC, FWF-40C, FG-50B, FG-50B-LENC, FWF-50B, FG-51B, FG-51B-LENC, FG-60B, FWF-60B, FG-60C, FG-60C-LENC, FWF-60C, FG-60C-POE, FG-60C-SFP, FWF-60CM. FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FG-80C, FG-80C-LENC, FG-80C-DC, FG-80CM, FWF-80CM, FWF-81CM, FG-82C, FG-100A, FG-100D, FG-100D-LENC, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-LENC, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-300C-LENC, FG-300C-DC, FG-310B, FG-310B-DC, FG-310B-LENC, FG-311B, FG-400A, FG-500A, FG-600C, FG-600C-DC, FG-600C-LENC, FG-620B, FG-620B-DC, FG-621B, FG-621B-DC, FG-800, FG-800C, FG-800C-DC, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, FG-1000C, FG-1000C-DC, FG-1000C-LENC, FG-1240B, FG-1240B-DC, FG-1240B-LENC, FG-3016B, FG-3040B, FG-3040B-DC, FG-3040B-LENC, FG-3140B, FG-3140B-DC, FG-3140B-LENC, FG-3240C, FG-3240C-DC, FG-3600, FG-3600A, FG-3810A, FG-3810A-DC, FG-3810A-LENC, FG-3950B, FG-3950B-DC, FG-3950B-LENC, FG-3951B, FG-3951B-DC, FG-5001, FG-5001A, FG-5001B, FG-5001C, FG-5001FA2, FG-5001FA2-LENC, FG-5002A, FG-5002A-LENC, FG-5002FB2, FG-5005FA2, FG-5101C FGR-100C FG-ONE FG-VM, FG-VM64, FG-VM64-XEN FS-5203B	v4.3

Table 7: Supported FortiCarrier models

Model	Firmware Version
FCR-3240C, FCR-3240C-DC, FCR-3600C, FCR-3600C-DC, FCR-3810A, FCR-3810A-DC, FCR-3950B, FCR-3950B-DC, FCR-3951B, FCR-3910B-DC, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	v5.2
FCR-3240C, FCR-3240C-DC, FCR-3600C, FCR-3600C-DC, FCR-3810A, FCR-3810A-DC, FCR-3950B, FCR-3950B-DC, FCR-3951B, FCR-3910B-DC, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	v5.0
FCR-3810A, FCR-3810A-DC, FCR-3950B, FCR-3950B-DC, FCR-3951B, FCR-3910B-DC, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	v4.3

Table 8: Supported FortiAnalyzer models

Model	Firmware Version
FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000B FAZ-VM, FAZ-VM64, FAZ-VM64-HV	v5.2
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 FAZ-VM, FAZ-VM64, FAZ-VM64-HV	v5.0

Table 9: Supported FortiMail models

Model	Firmware Version
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B FE-VM64	v5.1.3
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B FE-VM64	v5.0.6

Table 10: Supported FortiSandbox models

Model	Firmware Version
FSA-1000D, FSA-3000D	v1.4.0 and later v1.3.0 v1.2.0 and later

Table 11: Supported FortiSwitch ATCA models

Model	Firmware Version
FS-5003A, FS-5003B FTCL-5103B	v5.0.0
FS-5003A, FS-5003B	v4.3.0 v4.2.0

Table 12: Supported FortiWeb models

Model	Firmware Version
FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D FWB-VM64	v5.2.0 v5.1.4 v5.0.6

Table 13: Supported FortiCache models

Model	Firmware Version
FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D FCH-VM64	v3.0.0

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in v5.2.0.

Compatibility issues with FortiOS v5.2.1

The following table lists interoperability issues that have been identified with FortiManager v5.2.0 and FortiOS v5.2.1.

Table 14: Compatibility issues with FortiOS v5.2.1

Bug ID	Description
0254779	Install fails when creating a new VDOM.
0254804	Import fails if a VIP object protocol is configured as ICMP.
0254828	Install logs show warning messages for `profile-protocol-options` when `oversize-limit` settings are larger than `uncompressed-oversize-limit` settings.

Compatibility issues with FortiOS v5.2.0

The following table lists interoperability issues that have been identified with FortiManager v5.2.0 and FortiOS v5.2.0.

Table 15: Compatibility issues with FortiOS v5.2.0

Bug ID	Description
0227692	*Security Mode* > *Exempt List* support in *Network* > *Interfaces*.
0232983	User, User Group, and Device should be listed in the source or destination column.
0234563	The new VPN configuration wizard in FortiOS is not supported in FortiManager.

Compatibility issues with FortiOS v5.0.8 and v5.0.9

The following table lists interoperability issues that have been identified with FortiManager v5.2.0 and FortiOS v5.0.8 and v5.0.9.

Table 16: Compatibility issues with FortiOS v5.0.8 and v5.0.9

Bug ID	Description
0249560	The usb-wan related settings cannot be retrieved by FortiManager.
0252696	FortiManager should not add a mesh interface and a virtual AP when creating a VDOM.

Compatibility issues with FortiOS v5.0.5

The following table lists interoperability issues that have been identified with FortiManager v5.2.0 and FortiOS v5.0.5.

Table 17: Compatibility issues FortiOS v5.0.5

Bug ID	Description
0230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS v5.0.5 device causing the install to fail. FAP-320C is new for FortiOS v5.0.6.

Compatibility issues with FortiOS v5.0.4

The following table lists interoperability issues that have been identified with FortiManager v5.2.0 and FortiOS v5.0.4.

Table 18: Compatibility issues with FortiOS v5.0.4

Bug ID	Description
0226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS v5.0.5.
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 v5.0.5.
0226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS v5.0.5.
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 v5.0.5.
0226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS v5.0.5.
0230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS v5.0.4 device causing the install to fail. FAP-320C is new for FortiOS v5.0.6.

Resolved Issues

The following issues have been fixed in v5.2.0. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Table 19: Resolved device manager issues

Bug ID	Description
0204249	Import wizard should not allow user to map a single interface zone to a global zone that allows multiple interfaces.
0226318	Added `inbandwidth` configuration option to the advanced interface settings in FortiManager Web-based Manager.
0227533	Added new interface type: Virtual WAN.
0227666	*WiFi Templates* > *Custom AP Profiles* is missing FAP-320C support.
0231105	FortiManager may not be able to create a new VDOM.
0231602	After installing a global setting, the configuration status may still show pending or modified.
0232189	The policy ID filter does not function.
0232923	The ADOM and policy package list is updated when the ADOM is renamed resulting in no access to any ADOMs.
0234260	The FortiManager Web-based Manager displays the configuration status as *Out-Of-Sync* when a guest WiFi user is configured directly on FortiGate.
0234660	All policy package status changes to *Modified* when a new FortiGate is added into the same ADOM.
0236743	AntiVirus feature is now displayed in FortiGuard services list of the *License Information* widget when enabled.
0237692	The disk quota value is not saved after promoting a device.
0238121	Added support for FortiSandbox after upgrading to v1.2.3.
0238255	FortiManager generates a *web server Error500* when trying to edit a VLAN interface name with a space.
0238957	FortiManager's wireless AP profile is missing 802.11ac for FAP-320C and FAP-221C models.
0239214	The Endpoint Profile should allow users to select Web Filter Profiles and Application Sensor profiles.
0241542	Changes to the WiFi SSID page are not supported.

Table 19: Resolved device manager issues (continued)

Bug ID	Description
0244173	Users cannot discard custom replacement message changes leaving it blank.
0247034	FortiManager can no longer fully manage FortiGate device, showing the following error message after upgrading to v5.0.7: `You cannot access this device/VDOM`.
0247463	FortiManager prompts a `Web Server Error500` when editing a FortiGate's interface with the FortiManager in offline mode.
0247598	FortiManager may not be able to add a FortiOS Carrier device.
0247645	Search does not work for FSSO.
0247730	Using the right click menu from the source interface column to add a newly created address triggers an error message.
0248850	FortiManager cannot add an IP address for a DHCP relay on an interface.
0249790	When clicking *View* from the device dashboard, some local user configurations are missing.
0250073	System may consume high CPU resources when moving devices across different ADOMs.
0250301	Users are unable to edit VDOM Resource Usage with an error message.

Global ADOM

Table 20: Resolved Global ADOM issues

Bug ID	Description
0222978	In the Global *Policy Package*, the value for `auto-asic-offload` is set to disable instead of enable (default).
0236711	The `execute formatlogdisk` CLI command generates inconsistent outputs.
0239049	Assigning global policy package with *Automatically install policies to ADOM devices* is stuck at 50% during installation. Also, the ADOM policy package install in any ADOM is stuck at the *Validation* screen.
0240735	After installing global policies, the policy package status is not synchronized when the Global ADOM is unlocked.

Other

Table 21: Other resolved issues

Bug ID	Description
0222135	The `diagnose dvm device list` command incorrectly displays the package status.
0226155	The result of the changes made by the `objcfg-integrity` command is inconsistent.
0231959	Added support for SNMP OIDs in the FORTINET-CORE-MIB.
0232442	Locking/unlocking an ADOM does not change the read only/read write access for web portal.
0235706, 0237174	Resolved several XSS vulnerabilities issues.
0237447	When using XML web services, the full certificate chain is not generated.
0241669	FortiManager is not able to print dynamic mapping by `print-global-object`.
0242727	SDK and JSON may return *Firewall group is locked* and *No permission for the resource* errors.
0244410	Patched SSL/TLS MITM vulnerability (CVE-2014-0224).
0246074	HA may not be synchronized, and there is a show keep alive failure.
0247059	Resolved several SSH/SSL vulnerability issues.
0247189	Tunnel IP addresses to FortiGate can be exhausted.
0249801	Resolved a XSS injection issue in the Web-based Manager and Telnet.
0247599	The `diagnose test deploymanager reloadconf` command does not indicate the cause of a failure and the session terminates abruptly.

Policy and Objects

Table 22: Resolved policy and objects issues

Bug ID	Description
0212111	You can select one or multiple Dynamic IP Pools when you right-click the NAT policy cell in the FortiManager Web-based Manager.
0216116	Added *Packet Capture Configuration* option to the Access Control setting under Admin profile.
0223912	Section View is not available when a policy package is in a folder.
0223937	The section view of Policy Package is available after an upgrade to v5.0.5.
0227508	Web Filter advanced options are grouped in the FortiManager Web-based Manager.

Table 22: Resolved policy and objects issues (continued)

Bug ID	Description
0227632	The Virtual IP *Source Address Filter* in the Firewall Objects pane now uses a table list.
0227641	The Web-based Manager supports the new Virtual IP type `dns-translation`.
0231969	Device Selection menu is inconsistent between device level and policy package level Installs
0232603	FortiManager cannot delete real servers via the Web-based Manager.
0232891	Added the *Enable Replacement Messages for HTTP-based Applications* option in the Application Control setting under Security profiles.
0233140	Run time error when editing SSL/SSH inspection to enable inspect all ports.
0234094	*SSL VPN*, *Security*, and *Web Proxy* device profile entries are shown as not defined when a new device is added under the Replacement Message Group.
0234860	The Policy Package Install Wizard displays *no installing devices/no changes on package message* when rating overrides entries are installed in FortiGate.
0235815	Different search fields in a policy package may return different results when the query is the same.
0235934	Unable to install new Policy Package.
0236105	Unable to view comments column for *Address* under Firewall Objects.
0237033	The Web-Proxy policy should not support Capture Packets for logging.
0237137	When a user uses the *Where Used* feature in a firewall address object which is an IP range used within a SSL VPN portal, the result does not provide useful information.
0237228	Policy package service tool tips for ICMP/any does not show the type for the ICMP.
0237290	FortiManager returns JSON error when editing a shared address object of a policy.
0237441	Service group comments are not displayed in the FortiManager Web-based Manager.
0237520	ADOM *Revision Diff* feature displays inconsistent log settings.
0237635	Unable to view full text in the *Comments* column for Policy Package.
0238470	FortiManager cannot edit an existing or new *IPS Sensor* filter if there are more than 8192 entries.
0238547	*Policy Check* feature does not identify duplicate firewall address objects.
0238597	Dragging and dropping more than one scheduler into a policy should not be allowed.

Table 22: Resolved policy and objects issues (continued)

Bug ID	Description
0239348	*Where Used* command does not work when a firewall address name contains the ampersand character.
0239792	FortiManager fails to import firewall policies.
0243463	Auto-generated VPN zones do not show up when creating a policy.
0246482	One time schedule firewall object does not retain time settings once it is edited.
0247352	FortiManager should support new IPS statements from IPSE 2.991.
0247458	It is impossible to choose a value for the *Comments* and *Change_Request_number* column filters.
0247957	When searching for an IP address from firewall objects, if the group contains multiple matches, the search only highlights the first instance.
0247988	Dynamic mapping does not work for an address when the first octet is above 127.
0248019	It is impossible to unset the `session-ttl` value of a policy, and this change is pushed to the FortiGate device.
0248367	It is impossible to disable the traffic shaper option.
0248418	FortiManager does not allow spaces in the --pattern statement in an IPS custom signature.
0248776	When modifying a multicast policy, the fields should populate according to what is currently set.

Revision History

Table 23: Resolved revision history issues

Bug ID	Description
0226124	*Revision Diff* feature embeds extra space between words.
0234646	FortiManager is not able to install a secondary IP when using the Install Policy Package & Device settings.
0240464	Installation verification fails if a route is added or modified on FortiGate with the destination netmask in CIDR format.
0243939	Revision Diff highlights incorrect configuration changes.
0245257	After changing an identity policy to a normal policy, the policy package installation fails due to a incorrect *device-detection-portal* parameter.
0250353	FortiManager may delete VPN policies if some VPN tunnels are configured in tunnel mode.
0250442	Verification failed after configuring `vdom-property`.

Script

Table 24: Resolved script issues

Bug ID	Description
0215109	When creating a default route via script, FortiManager defines default gateway as 255.255.255.255.
0223194	A custom service in Policy Package should be created via a script if it contains incorrect value for the protocol number.
0232762	All subsequent Tcl scripts fail to execute after a script failed and aborted.
0233183	Hexadecimal data should not be case sensitive.
0237944	FortiManager fails to run a script to delete a VLAN interface.
0239243	FortiManager is unable to install Global Policies imported via a script.
0246699	The `getScriptLog` API always returns last executed script.

Services

Table 25: Resolved services issues

Bug ID	Description
0243842	Oracle proxy server does not support some `User-Agent` information in FortiManager.
0247268	If there are no custom URLs during an export, the FortiManager should either display a proper error message or export a blank file.
0249397	The update timer is inconsistent with update history.

System Settings

Table 26: Resolved system settings issues

Bug ID	Description
0217785	The default *Task Monitor* list size value in FortiManager should be increased.
0217785	FortiManager should increase the default task list size value.
0217786	Added a CLI option to modify task list size.
0228117	Some JSON locking events are not stored in event logs.
0228841	Cannot bind a LDAP server on a specific ADOM.
0231372	The Admin ADOM name is not updated when the corresponding ADOM name is changed.
0234856	When running a script with BGP settings, FortiManager needs to populate initial BGP configurations on a device.
0235003	FortiManager cannot create an IPv6 BGP neighbor via script.

Table 26: Resolved system settings issues (continued)

Bug ID	Description
0237988	Downloaded certificate request includes HTTP header data.
0246504	Increased the key length of the TACACS+ server used by FortiManager to 128 characters.
0247840	A user with read-only access should not be allowed to change their password.

Known Issues

The following issues have been identified in v5.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Table 27: Known device manager issues

Bug ID	Description
0250086	Double clicking a VDOM does not highlight it in the device tree.
0252558	Unable to display Central VPN query data.

Other

Table 28: Other known issues

Bug ID	Description
0251709	Browser tab closes after installed or imported a policy package.

Policy and Objects

Table 29: Known policy and objects issues

Bug ID	Description
0249905	Validation should be done when adding a service in a policy with drag and drop.
0251156	Per-user black white list (BWL) is not visible on FortiManager.
0251349	After an ADOM is upgraded to v5.0, SCTP anomalies are missing from DOS policies.

Script

Table 30: Known script issues

Bug ID	Description
0251352	It is possible to create a LAG interface via a script with member interfaces already mapped and used in policy.

Services

Table 31: Known services issues

Bug ID	Description
0251173	After manually uploaded an IPS Engine, it is not listed under FortiGuard Package Management.

System Settings

Table 32: Known system settings issues

Bug ID	Description
0251713	SQL error messages are logged to the event log when deleting a policy package.

Appendix A: FortiGuard

FortiGuard Distribution Servers (FDS) and services

In order for the FortiManager to request and retrieve updates from FortiGuard Distribution Servers, 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. FortiManager 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 v5.2.0 as a local FortiGuard Distribution Server (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:

Table 33: FortiGuard Center update support

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	• v5.0.0 and later • v5.2.0 and later	✔		✔	
FortiClient (Windows)	• v4.3.0 and later	✔			
FortiClient (Windows)	• v4.2.0 and later	✔	✔		✔
FortiClient (Mac OS X)	• v5.0.1 and later	✔		✔	
FortiMail	• v4.2.0 and later • v4.3.0 and later • v5.0.0 and later • v5.1.0 and later • v5.2.0 and later	✔	✔		

Table 33: FortiGuard Center update support (continued)

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiSandbox	• v1.2.0, v1.2.3 • v1.3.0 • v1.4.0 and later	✔			
FortiWeb	• v5.0.6 • v5.1.4 • v5.2.0 and later • v5.3.0	✔			

To enable FortiGuard Center updates for FortiMail v4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
  set status enable
end
```