FortiManager v5.0 Patch Release 6

Release Notes

FortiManager v5.0 Patch Release 6 Release Notes

May 13, 2014

02-506-225563-20140513

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 **5**

Introduction **6**

Supported models 6

FortiManager 6

FortiManager VM 6

Summary of enhancements 7

Special Notices **8**

FortiManager VM 8

Unregistered device table 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

ADOM for FortiMail or FortiWeb 9

FortiOS v5.0 override server setting for FortiGuard Services 10

Example 1: Antivirus/IPS 10

Example 2: Web filtering/Antispam 10

Update services provided to FortiGate v4.0 MR2 or FortiMail devices 11

Log arrays 11

Endpoint management 11

FortiManager VM license check 12

Multi-language display support 12

New hard disk drive partition layout 12

Importing a FortiManager generated policy 12

Importing profile group and RADIUS dynamic start server 12

Push update in bi-directional static NAT 13

Upgrade Information **14**

Upgrading from FortiManager v5.0.0 or later 14

Upgrading from FortiManager v4.0 MR3 14

General firmware upgrade steps 15

Downgrading to previous firmware versions 19

FortiManager VM firmware 19

Firmware image checksums 19

Product Integration and Support **20**

Web browser support 20

FortiOS support 20
FortiOS Carrier support 20
FortiAnalyzer support 21
FortiMail support 21
FortiWeb support 21
FortiSwitch ATCA support 21
FortiClient support 21
FortiSandbox support 21
Virtualization software support 22
Feature support 22
Language support 22
Supported models 23
Compatibility with FortiOS Versions 26
FortiOS features currently not supported by FortiManager 26
Compatibility issues with FortiOS v5.0 Patch Release 5 26
Compatibility issues with FortiOS v5.0 Patch Release 4 26
Resolved Issues 28
Device Manager 28
Global ADOM 28
High Availability 29
Other 29
Policy and Objects 29
Revision History 30
Script 30
VPN Console 30
Known Issues 31
Device Manager 31
Other 31
Revision History 31
System Settings 32
Upgrade 32
Appendix A: FortiGuard 33
FortiGuard Distribution Servers (FDS) and services 33
FortiGuard Center update support 33

Change Log

Date	Change Description
2014-02-05	Initial release.
2014-02-11	Added 0231686 and 0231703 to Table 22. Added 0230199 to Table 13.
2014-02-12	Added FCTL-5103B to Table 10.
2014-03-03	Added feature support table and updated FortiGuard support table.
2014-03-07	Added FMG-4000E to supported models.
2014-04-04	Added 0225862 and 0228169 to Table 14.
2014-04-15	Added FortiOS and FortiOS Carrier v5.0 Patch Release 7 to Product Integration and Support.
2014-04-21	Updated support model tables.
2014-05-13	Added 0234819 to Table 26

Introduction

This document provides a summary of enhancements, support information, installation instructions, integration, resolved and known issues in FortiManager v5.0 Patch Release 6 build 0310. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiManager device, see the *FortiManager Administration Guide*.

This document incudes the following sections:

- Introduction
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- FortiGuard

Supported models

The following models are supported on FortiManager v5.0 Patch Release 6.

FortiManager

FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, and FMG-5001A.

FMG-4000E

This model is released on a special branch based off of FortiManager v5.0 Patch Release 6. As such, the build number found in the *System* > *Dashboard* page and the output from the `get system status` CLI command displays `4046` as the build number.

FortiManager VM

FMG-VM32, FMG-VM64, and FMG-VM64-HV.

See the Fortinet Document Library for additional FortiManager v5.0 documentation.

Summary of enhancements

The following is a list of enhancements in FortiManager v5.0 Patch Release 6:

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

- High Availability re-synchronization improvements
- Support FG-1500D and FG-3700D
- Support FortiSandbox in a separate ADOM
- Policy package locking (independent of ADOM lock)
- Import improvements
- Central WiFi management improvements
- FortiManager VM supports up to 12 virtual disks (LVM)

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiManager v5.0 Patch Release 6 build 0310.

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.

Unregistered device table

In FortiManager v5.0 Patch Release 4 or earlier releases, the `config system global set unregister-pop-up` command is enabled by default. When a device is configured to send logs to FortiManager, the unregistered device table will be displayed. You can decide to promote the device now or at a later date.

In FortiManager v5.0 Patch Release 5 or later, the `config system global set unregister-pop-up` command is disabled by default. When a device is configured to send logs to FortiManager, the unregistered device table will not be displayed. Instead, a new entry *Unregistered Devices* will appear in the Device Manager tab under *All FortiGate*. You can then promote devices to specific ADOMs or use the right-click menu to delete the device.

Figure 1: Promote unregistered devices

FortiAnalyzer feature set

In FortiManager v5.0 Patch Release 5 or later, the FortiAnalyzer feature set (Log View, Drill Down, Event Management, and Reports) is disabled by default. To enable these features, 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.

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 (Microsoft Hyper-V).

ADOM for FortiCarrier

Please note that FortiGate and FortiCarrier devices can no longer be grouped into the same ADOM in FortiManager v5.0 Patch Release 6. 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.

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

ADOM for FortiMail or FortiWeb

In order for FortiMail or FortiWeb devices to be promoted to the DVM table, Administrative Domain must be enabled in *System Settings* > *System Information*. FortiMail and FortiWeb devices are added to device specific ADOMs.

You cannot add FortiMail or FortiWeb devices to FortiManager using the Add Model Device option in the Add Device wizard.

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 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. Table 1 lists the ports used by FortiGuard Services.

Table 1: 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 FortiGuard uses port 443 to provide antivirus/IPS updates. On 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.

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:

```
10.1.100.2:8890 -> 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 FortiGate v4.0 MR2 or FortiMail devices

Please enable the following option in order to provide update services to FortiGate v4.0 MR2 and FortiMail devices:

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

Log arrays

After creating a log array, only new logs will be populated into this array. Older logs will remain on the device. To collect older logs, you will need to build the array database. Use the following CLI command to build the array database:

```
execute sql-local rebuild-device <log array device ID>
```

The SQL logs for the members of the log array will be rebuilt. To verify that the array rebuild was successful, select the *Log View* tab to view the log array and logs.

Executing this command will not reboot the FortiManager device.

Fortinet recommends configuring log arrays prior to deploying the FortiManager into production. When adding and deleting log arrays, you will need to rebuild the database to view older logs.

Endpoint management

In version 5.0, 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 5.0 Handbook* available in the Fortinet Document Library.

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 v5.0 Patch Release 1 or later has restrictions on supporting a FortiGate device's multi-language display.

New hard disk drive partition layout

FortiManager v5.0.0 introduced a new hard disk drive partition layout which is required for optimal usage and performance. Following an upgrade to FortiManager v5.0.0 or later, a backup must be made and then the disk must be reformatted with following command:

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

A format will erase all local logs, and FortiGuard database information. Backup any local event logs that you wish to keep. The FortiManager will then need to re-download all of the AV/IPS/AS/WF objects from the FortiGuard Distribution Servers (FDS) which may take up to half a day. During that time managed devices will not be able to obtain these services from the FortiManager. You should configure devices to point to a backup FortiManager or the FDS for these services.

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

This section explains how to properly upgrade to FortiManager v5.0 Patch Release 6. The following topics are included in this section:

- Upgrading from FortiManager v5.0.0 or later
- Upgrading from FortiManager v4.0 MR3
- General firmware upgrade steps
- Downgrading to previous firmware versions

Please review the Special Notices, Product Integration and Support, and Known Issues chapters prior to upgrading. For more information on upgrading your FortiManager device, see the *FortiManager v5.0 Patch Release 6 Administration Guide* available at the Fortinet Document Library.

You can download the FortiManager MIB file in the firmware image FTP directory. The Fortinet Core MIB file is located in the main FortiManager v5.00 directory.

Upgrading from FortiManager v5.0.0 or later

FortiManager v5.0 Patch Release 6 build 0310 officially supports upgrade from FortiManager v5.0.0 or later.

Upgrading from FortiManager v4.0 MR3

FortiManager v5.0 Patch Release 6 build 0310 officially supports upgrade from FortiManager v4.0 MR3.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

Table 2: Upgrade steps

Step 1	Prepare your FortiManager for upgrade.
Step 2	Backup your FortiManager system configuration. For FortiManager VM, take a *Snapshot* of the VM instance.
Step 3	Transfer the FortiManager firmware image to your FortiManager device.
Step 4	Log into your FortiManager Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiManager for upgrade

1. Install any pending configurations.
2. Make sure all managed devices are running the supported firmware versions as stated in "Product Integration and Support" on page 20.
3. Download the firmware image from the Customer Service & Support portal.
4. Verify the integrity of the image using the *Firmware Image Checksums* tool.

Step 2: Backup your FortiManager system configuration

1. Go to *System Settings* > *Dashboard*.
2. Select *Backup* in the *System Information* widget.

   The *Backup* dialog box opens.

   Figure 2: Backup dialog box

3. Select the checkbox to encrypt the backup file and enter a password.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiManager device.

4. Select *OK* and save the backup file on your management computer.

The system configuration file from a FortiManager v4.0 MR3 device cannot be directly imported into a FortiManager v5.0 Patch Release 6 device.

Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename save to
     the server> <username on server> < password> <crptpasswd>
execute backup all-settings scp <server IP address> <path/filename
     save to the server> <SSH certificate> <crptpasswd>
```

For more information, see the *FortiManager v5.0 Patch Release 6 CLI Reference* available in the Fortinet Document Library.

5. In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

Figure 3: Snapshot of FortiManager VM (VMware)

For information on snapshots in Microsoft Hyper-V Server environments, refer to the Microsoft Windows Server online help.

Figure 4: Snapshot of FortiManager VM (Microsoft Hyper-V)

Step 3: Transfer the firmware image to your FortiManager device

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

   The *Firmware Update* dialog box opens.

   Figure 5: Firmware upgrade dialog box

3. Select *Browse* to locate the firmware image (`.out` file) that you downloaded from the Customer Service & Support portal and select *Open*.
4. Select *OK*. Your FortiManager will upload the firmware image and you will receive the following message.

Figure 6: Firmware upgrade successful dialog box

Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to the server> <server
     ip address> <username on server> <password>
```

For more information, see the *FortiManager v5.0 Patch Release 6 CLI Reference* available in the Fortinet Document Library.

Step 4: Verify the upgrade

1. Refresh the browser and log back into the device.

After the upgrade, please clear your browser cache before logging into the FortiManager Web-based Manager. Please make sure your computer's screen resolution is set to at least 1280x1024, otherwise the Web-based Manager may not be displayed properly.

2. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
3. Select each ADOM and make sure that managed devices reflect the appropriate connectivity state. Optionally, go to *System Settings* > *All ADOM*s.

Figure 7: Verify device connectivity

4. Launch other functional modules and make sure they work properly.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous FortiManager firmware release via the Web-based Manager or CLI. A system reset is required after the firmware downgrading process has completed.

All configuration will be lost after downgrading the device. For FortiManager devices with hard drives installed, the hard drives will be formatted.

To re-initialize a FortiManager 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.

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.

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.

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

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*.

Product Integration and Support

Web browser support

FortiManager v5.0 Patch Release 6 supports the following web browsers:

- Microsoft Internet Explorer versions 10 and 11
- Mozilla Firefox version 28
- Google Chrome version 34

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiManager v5.0 Patch Release 6 supports the following FortiOS versions:

- v5.0 Patch Release 7
- v5.0 Patch Release 6
- v5.0 Patch Release 5

  FortiManager v5.0 Patch Release 6 is fully tested as compatible with FortiOS v5.0 Patch Release 5, with some minor compatibility issues. For more information, see "Compatibility with FortiOS Versions" on page 26.
- v5.0 Patch Release 4

  FortiManager v5.0 Patch Release 6 is fully tested as compatible with FortiOS v5.0 Patch Release 4, with some minor compatibility issues. For more information, see "Compatibility with FortiOS Versions" on page 26.
- v4.0 MR3 and Patch Release 2 or later
- v4.0 MR2 and Patch Releases

FortiOS Carrier support

FortiManager v5.0 Patch Release 6 supports the following FortiOS Carrier versions:

- v5.0 Patch Release 7
- v5.0 Patch Release 6
- v5.0 Patch Release 5

  FortiManager v5.0 Patch Release 6 is fully tested as compatible with FortiOS Carrier v5.0 Patch Release 5, with some minor compatibility issues. For more information, see "Compatibility with FortiOS Versions" on page 26.
- v5.0 Patch Release 4

  FortiManager v5.0 Patch Release 6 is fully tested as compatible with FortiOS Carrier v5.0 Patch Release 4, with some minor compatibility issues. For more information, see "Compatibility with FortiOS Versions" on page 26.
- v4.0 MR3 and Patch Release 2 or later
- v4.0 MR2 and Patch Releases

FortiAnalyzer support

FortiManager v5.0 Patch Release 6 supports the following FortiAnalyzer versions:

- v5.0 and all Patch Releases
- v4.0 MR3 and all Patch Releases
- v4.0 MR2 and all Patch Releases

FortiMail support

FortiManager v5.0 Patch Release 6 supports the following FortiMail versions:

- v5.0 MR1
- v5.0 Patch Release 3

FortiWeb support

FortiManager v5.0 Patch Release 6 supports the following FortiWeb versions:

- v5.0 MR1 Patch Release 1
- v5.0 Patch Release 5

FortiSwitch ATCA support

FortiManager v5.0 Patch Release 6 supports the following FortiSwitch ATCA versions:

- v5.0.0 and Patch Releases
- v4.0 MR3 and Patch Releases
- v4.0 MR2 and Patch Releases

FortiClient support

FortiManager v5.0 Patch Release 6 supports the following FortiClient versions:

- FortiClient (Windows) v5.0 Patch Release 4 or later
- FortiClient (Mac OS X) v5.0 Patch Release 4 or later

FortiSandbox support

FortiManager v5.0 Patch Release 6 supports the following FortiSandbox version:

- FortiSandbox v1.0 MR2

Virtualization software support

FortiManager v5.0 Patch Release 6 supports the following virtualization software:

- VMware ESX versions 4.0 and 4.1
- VMware ESXi versions 4.0, 4.1, 5.0, 5.1, and 5.5
- Microsoft Hyper-V Server 2008 R2 and 2012

Feature support

The following table lists feature support for managed platforms.

Table 3: Feature support per platform

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

Language support

The following table lists FortiManager language support information.

Table 4: FortiManager language support

Language	Web-based Manager	Reports	Documentation
English	✔	✔	✔
French	-	✔	-
Spanish (Spain)	-	✔	-
Portuguese (Brazil)	-	✔	-
Korean	✔	✔	-
Chinese (Simplified)	✔	✔	-
Chinese (Traditional)	✔	✔	-
Japanese	✔	✔	-

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch, and FortiWeb models and firmware versions that can be managed by a FortiManager appliance running FortiManager v5.0 Patch Release 6.

Table 5: Supported FortiGate models

Model	Firmware Version
FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60D, FG-60D-POE, FG-60D-3G4G-VZW, FG-80C, FG-80CM, FG-90D, FG-90D-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-280D-POE, FG-300C, FG-310B, FG-310B-DC, FG-311B, FG-600C, FG-620B, FG-620B-DC, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5101C FGR-100C FG-VM32, FG-VM64, FG-VM64-AWS, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN 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-80CM FWF-81CM, FWF-90D, FWF-90D-POE FS-5203B	v5.0
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-310B-DC, FG-311B, FG-400A, FG-500A, FG-600C, FG-620B, FG-620B-DC, FG-621B, FG-800, FG-800C, FG-800F, FG-1000, FG-1000A, FG-1000A-FA2, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001C, FG-5001FA2, FG-5002FB2, FG-5005FA2, FG-5101C, FG-ONE FGR-100C FG-VM32, FG-VM64, FG-VM64-XEN 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 FS-5203B	v4.0 MR3

Table 5: Supported FortiGate models (continued)

Model	Firmware Version
FG-30B, FG-50B, FG-51B, FG-60-ADSL, FG-60B, FG-60C, FG-60CM, FG-80C, FG-80CM, FG-82C, FG-100A, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-310B-DC, FG-311B, FG-400A, FG-500A, FG-620B, FG-620B-DC, FG-621B, FG-800, FG-800F, FG-1000, FG-1000A, FG-1000A-FA2, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001FA2, FG-5002FB2, FG-5005FA2, FG-ONE FG-VM FWF-30B, FWF-50B, FWF-60B, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM	v4.0 MR2

Table 6: Supported FortiCarrier models

Model	Firmware Version
FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	v5.0
FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	v4.0 MR3
FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	v4.0 MR2

Table 7: Supported FortiAnalyzer models

Model	Firmware Version
FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B FAZ-VM, FAZ-VM64, FAZ-VM64-HV	v5.0
FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B	v4.0 MR3, v4.0 MR2

Table 8: 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	v5.0 MR1
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 Patch Release 3

Table 9: Supported FortiSandbox models

Model	Firmware Version
FSA-1000D, FSA-3000D	v1.0 MR2

Table 10: Supported FortiSwitch ATCA models

Model	Firmware Version
FTCL-5103B, FS-5003A, FS-5003B	v5.0
FS-5003A, FS-5003B	v4.0 MR3, v4.0 MR2

Table 11: 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-VM	v5.0 MR1 Patch Release 1
FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D FWB-VM	v5.0 Patch Release 5

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager v5.0 Patch Release 6 build 0310.

FortiOS features currently not supported by FortiManager

The following features in FortiOS v5.0 Patch Release 5 are not supported in FortiManager v5.0 Patch Release 6:

- Updated categories within the application sensor
- Mobile FortiToken support
- FortiManager should support SSL VPN custom login
- SSL VPN custom login support
- Add *More Filters* options for IPS and Application Control profiles
- Add Web Filter administrative override Web-based Manager support

Compatibility issues with FortiOS v5.0 Patch Release 5

The following table lists known interoperability issues that have been identified with FortiManager v5.0 Patch Release 6 and FortiOS v5.0 Patch Release 5.

Table 12: Compatibility issues

Bug ID	Description
0230199	FortiManager allows the creation of a new FAP320C WTP profile on a FortiOS v5.0 Patch Release 5 device causing the install to fail. FAP320C is new for FortiOS v5.0 Patch Release 6.

Compatibility issues with FortiOS v5.0 Patch Release 4

The following table lists known interoperability issues that have been identified with FortiManager v5.0 Patch Release 6 and FortiOS v5.0 Patch Release 4.

Table 13: Compatibility issues

Bug ID	Description
0226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS v5.0 Patch Release 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 Patch Release 5.

Table 13: Compatibility issues (continued)

Bug ID	Description
0226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS v5.0 Patch Release 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 Patch Release 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 Patch Release 5.
0230199	FortiManager allows the creation of a new FAP320C WTP profile on a FortiOS v5.0 Patch Release 4 device causing the install to fail. FAP320C is new for FortiOS v5.0 Patch Release 6.

Resolved Issues

The resolved issues tables listed below do not list every bug that has been corrected with FortiManager v5.0 Patch Release 6 build 0310. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Table 14: Resolved device manager issues

Bug ID	Description
0191127	FortiManager cannot upgrade FortiAP firmware from the FortiManager Web-based Manager.
0216556	Import of a v5.0 FortiGate configuration into v4.0 MR3 ADOM causes the security console daemon to crash and install wizard hangs.
0216679	The deauthorize button should not be available for a FortiWiFi which has local WiFi capability.
0217458	There are inconsistencies when creating transparent mode VDOMs via the right click menu and the VDOM tab.
0225862	Copy performance improvements. Copy should not skip modified devices.
0226026	Connectivity refresh results in an internal error and `dvmcmd` crash.
0227872	Device's contact, country, city, province and company information is not displayed from *Device Group* view.
0228169	An install, no change, reinstall results in a *no installing devices* error.
0228427	Remove FortiGate related columns in the FortiMail summary page.

Global ADOM

Table 15: Resolved Global ADOM issues

Bug ID	Description
0227516	After creating the custom service ALL, Global Policy Package assignment fails with the error *Device level already has object objcfg_fw_srv_cus:ALL*.

High Availability

Table 16: Resolved HA issues

Bug ID	Description
0173017	All slave units in a FortiManager HA cluster resynchronize when a slave joins the master.
0173018	The `diagnose ha force-resync` CLI command causes all slave units to resynchronize.
0223577	The unregister-pop-up setting is not synced from master to slave.
0226511	When a slaves joins or re-joins a cluster, it needs to do a full synchronization with the master. A slave should not be promoted to master unless this synchronization is complete or the hard disk of the slave is reformatted.

Other

Table 17: Other resolved issues

Bug ID	Description
0194590	The current `diagnose cdb check objcfg-integrity` CLI command does not indicate which changes will be made.
0227140	Administrator policy package settings are not synchronized to the FortiManager slave unit.
0228827	`fmgd` segmentation fault during an install operation.

Policy and Objects

Table 18: Resolved policy and objects issues

Bug ID	Description
0180983	The user group option becomes unselected when creating a new FortiClient VPN.
0184537	The captive portal disclaimer maximum size does not match that on FortiGate.
0220727	FortiManager should not allow drag and drop of a policy package to another package.
0223945	FortiManager allows adding device and gateway to FortiGate's blackhole routes.
0224075	FortiManager cannot handle the `os-check-listatest-patch-level` attribute properly for SSL VPN portal.
0225068	FortiManager deletes FortiToken users from FortiGate.
0225274	In a v4.0 MR2 ADOM, device level retrieve and ADOM level refresh should work for the FSAE user list.

Table 18: Resolved policy and objects issues (continued)

Bug ID	Description
0227147	FortiManager is not able to create an address when adding members in an address group.
0227749	A one-time scheduled object cannot be created for the 31th of a month.
0227769	ADOM policy does not support destination VIPs binding to a zone which is assigned with different interface members.
0228112	Firewall policy copy fails because of incorrect firewall *profile-protocol-options* NNTP protocol settings.
0228268	The policy package installation preview is blank when it takes a long time to load.
0228567	Added a progress bar for device installation preview.

Revision History

Table 19: Resolved revision history issues

Bug ID	Description
0225059	FortiManager tries to set ssl-xxx parameters on FortiGate's VIP settings resulting in an install verification failure.

Script

Table 20: Resolved script issues

Bug ID	Description
0210962	CLI script error messages are not descriptive about subnet error.
0227747	FortiManager prompts a script error when the target is *Run on Policy Package*, *ADOM Database or Global Policy,* and *Advanced Device Filters* is used.

VPN Console

Table 21: Resolved VPN console issues

Bug ID	Description
0226405	Improved performance to display a bulk of devices.
0227284	VPN Console does not display FortiGates' names in alphabetical order.
0228090	Added support in VPN Console to allow multiple VDOMs of same device in single VPN.

Known Issues

The known issues tables listed below do not list every bug that has been identified with FortiManager v5.0 Patch Release 6 build 0310. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Table 22: Known device manager issues

Bug ID	Description
0229088	FortiManager shows the wrong device when choosing a particular member from a FortiGate device group.
0229606	VDOMs associated with an unregistered device are unexpectedly displayed under *All FortiGates*.
0229635	FortiManager prompts an error when modifying the soft switch with only one interface member.
0229738	FortiManager is not able to create two dead gateway detection profiles for the same interface.
0229894	FortiManager incorrectly modifies the policy package status following an auto update.
0231686	Configuration and install status is incorrect if ADOM is unlocked and settings are not saved after assigning a provisioning template without an install.
0231703	After a policy package re-install, the CLI always shows policy package status as modified instead of installed.

Other

Table 23: Other known issues

Bug ID	Description
0229188	An install operation from the web portal does not push changes to FortiGate.

Revision History

Table 24: Known revision history issues

Bug ID	Description
0231157	Verification may fail on replacement messages when installing to a FortiCarrier device.

System Settings

Table 25: Known system settings issues

Bug ID	Description
0229514	FortiManager is unable to restore an encrypted backup file in the Web-based Manager if the password contains more than 14 characters.
0230251	*AutoSync*, *AutoUpdate*, and *AutoRetrieve* terminology inconsistencies.
0230399	Event log entry for *AutoRetrieve* is not consistent with that of *AutoUpdate* and *AutoSync*.
0230568	FortiManager generates unexpected configuration change event logs when a device's configuration is not modified.

Upgrade

Table 26: Known upgrade issues

Bug ID	Description
0234819	The firewall service `ICMP_ANY` is removed from policy after an ADOM upgrade.

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 v5.0 Patch Release 6 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 27: FortiGuard Center update support

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	v5.0.0 or later	✔		✔	
FortiClient (Windows)	v4.0 MR3	✔			
FortiClient (Windows)	v4.0 MR2	✔	✔		✔
FortiClient (Mac OS X)	v5.0.1or later	✔		✔	
FortiMail	v4.0 MR2, v4.0 MR3, v5.0	✔	✔		
FortiSandbox	v1.0 MR2	✔			

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

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