



# FortiManager - Release Notes

**VERSION 5.2.7**

**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](mailto:techdocs@fortinet.com)



April 8, 2016

FortiManager 5.2.7 Release Notes

02-527-366756-20160408

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
Supported models	6
<b>Special Notices</b>	<b>7</b>
Limitation on backing up and restoring FortiManager's Database	7
Hyper-V FortiManager-VM running on an AMD CPU	7
Multicast Policy Support at ADOM Level	7
ADOM for FortiGate 4.2 Devices	7
SSLv3 on FortiAnalyzer-VM64-AWS	7
SQL database rebuild	8
Web Portal support	8
CLI commands for configuring dynamic objects	8
FortiManager VM	9
FortiAnalyzer feature set	9
FortiGate firmware upgrade	9
System time on FortiManager VM	10
Memory requirement for FortiManager VM64-HV	10
ADOM for FortiCarrier	10
FortiOS 5.0 override server setting for FortiGuard Services	10
Example 1: Antivirus/IPS	11
Example 2: Web filtering/Antispam	11
Update services provided to FortiMail 4.2 devices	11
Endpoint management	12
FortiManager VM license check	12
Multi-language display support	12
Importing a FortiManager generated policy	12
Importing profile group and RADIUS dynamic start server	12
Push update in bi-directional static NAT	13
<b>Upgrade Information</b>	<b>14</b>
Upgrading to FortiManager 5.2.7	14
Downgrading to previous firmware versions	14
FortiManager VM firmware	14

Firmware image checksums .....	15
SNMP MIB files .....	15
<b>Product Integration and Support .....</b>	<b>16</b>
FortiManager 5.2.7 support .....	16
Feature support .....	18
Language support .....	18
Supported models .....	19
<b>Compatibility with FortiOS Versions .....</b>	<b>26</b>
Compatibility issues with FortiOS 5.2.7 .....	26
Compatibility issues with FortiOS 5.2.3 .....	26
Compatibility issues with FortiOS 5.2.1 .....	26
Compatibility issues with FortiOS 5.2.0 .....	27
Compatibility issues with FortiOS 5.0.5 .....	27
Compatibility issues with FortiOS 5.0.4 .....	27
<b>Resolved Issues .....</b>	<b>29</b>
Device Manager .....	29
Revision History .....	29
Services .....	29
<b>Known Issues .....</b>	<b>30</b>
AP Management .....	30
Services .....	30
System Settings .....	30
<b>FortiGuard Distribution Servers (FDS) .....</b>	<b>31</b>
FortiGuard Center update support .....	31

## Change Log

Date	Change Description
2016-04-08	Initial release.
2016-04-04	Updated the Multicast Policy Support at ADOM Level special notice and the Upgrade Information section to include information about invalid dynamic mappings and duplicate package settings being removed from the ADOM database.

# Introduction

This document provides the following information for FortiManager 5.2.7 build 757:

- [Supported models on page 6](#)
- [Special Notices on page 7](#)
- [Upgrade Information on page 14](#)
- [Product Integration and Support on page 16](#)
- [Compatibility with FortiOS Versions on page 26](#)
- [Resolved Issues on page 29](#)
- [Known Issues on page 30](#)
- [FortiGuard Distribution Servers \(FDS\) on page 31](#)

For more information on upgrading your device, see the FortiManager 5.2.7 Upgrade Guide.

## Supported models

FortiManager version 5.2.7 supports the following models:

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

## Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.2.7.

### Limitation on backing up and restoring FortiManager's Database

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

### Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel based PC.

### Multicast Policy Support at ADOM Level

Starting from FortiManager 5.2.2, configuration for multicast policy has been moved from individual FortiGate devices to an ADOM database. After upgrading, you can import multicast policies into the ADOM database by performing an "import policy" on all managed devices that have multicast policies configured. Otherwise, the FortiManager will delete all existing multicast policies on the FortiGate when installing a policy package.

### ADOM for FortiGate 4.2 Devices

FortiManager 5.2 no longer supports FortiGate 4.2 devices. FortiManager cannot manage the devices after the upgrade. To continue managing those devices, please upgrade all FortiGate 4.2 devices to a supported version; retrieve the latest configuration from the devices; and move the devices to an ADOM database with the corresponding version.

### SSLv3 on FortiAnalyzer-VM64-AWS

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

```
config system global
  set ssl-protocol tlsv1
end
```

## SQL database rebuild

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

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

## Web Portal support

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

## CLI commands for configuring dynamic objects

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

### Example 1: Dynamic VIP

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

### Example 2: Dynamic Address

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

### Example 3: Dynamic Interface

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

## FortiManager VM

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

## FortiAnalyzer feature set

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

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

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



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



In version 5.2.7, you can enable the FortiAnalyzer feature set in the Web-based Manager. Go to *System Settings > Dashboard*. In the *System Information* widget, beside *FortiAnalyzer Features*, select *Enabled*.

## FortiGate firmware upgrade

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

## System time on FortiManager VM

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

## Memory requirement for FortiManager VM64-HV

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

## ADOM for FortiCarrier

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

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



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

## FortiOS 5.0 override server setting for FortiGuard Services

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



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

### Ports used by FortiGuard services

Port	Service
8890	Antivirus or IPS updates for FortiGate

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

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

### Example 1: Antivirus/IPS

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

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

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

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

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

### Example 2: Web filtering/Antispam

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

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

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

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

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

## Update services provided to FortiMail 4.2 devices

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

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

## Endpoint management

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

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

## FortiManager VM license check

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

## Multi-language display support

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

## Importing a FortiManager generated policy

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

- Global Header Policy
- Global Footer Policy
- VPN Console

## Importing profile group and RADIUS dynamic start server

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

## Push update in bi-directional static NAT

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

Configure the following settings on FortiManager:

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

# Upgrade Information

## Upgrading to FortiManager 5.2.7

For information about upgrading your FortiManager device to 5.2.7, see *FortiManager 5.2.7 Upgrade Guide*.



During upgrade from 5.2.4 or earlier, invalid dynamic mappings and duplicate package settings are removed from the ADOM database. Please allow sufficient time for the upgrade to complete.

## Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

## FortiManager VM firmware

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

### Amazon Web Services

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

### Citrix XenServer and Open Source XenServer

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

### Linux KVM

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

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



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtualappliances.html>. VM installation guides are available in the [Fortinet Document Library](#).

---

## 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 5.2.7 support

The following table lists 5.2.7 product integration and support information:

<b>Web Browsers</b>	<ul style="list-style-type: none"> <li>• Microsoft Internet Explorer™ 11.0</li> <li>• Mozilla Firefox version 45</li> <li>• Google Chrome version 49</li> </ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p> <p>Please make sure your computer's screen resolution is set to at least 1280x1024. Otherwise, web pages may not be displayed properly.</p>
<b>FortiOS/FortiOS Carrier</b>	<p>FortiManager 5.2.7 expects to support the following versions:</p> <ul style="list-style-type: none"> <li>• 5.2.7           <p>FortiManager 5.2.7 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see <a href="#">Compatibility with FortiOS Versions on page 26</a>.</p> </li> <li>• 5.2.2 to 5.2.6</li> <li>• 5.2.1           <p>FortiManager 5.2.7 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see <a href="#">Compatibility with FortiOS Versions on page 26</a>.</p> </li> <li>• 5.2.0           <p>FortiManager 5.2.7 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues. For information, see <a href="#">Compatibility with FortiOS Versions on page 26</a>.</p> </li> <li>• 5.0.4 to 5.0.13           <p>FortiManager 5.2.7 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.13, with some minor interoperability issues. For information, see <a href="#">Compatibility with FortiOS Versions on page 26</a>.</p> </li> <li>• 4.3.2 to 4.3.18           <p>For the latest information, see FortiOS and FortiManager Compatibility at <a href="http://docs.fortinet.com/d/fortimanager-compatibility">http://docs.fortinet.com/d/fortimanager-compatibility</a></p> </li> </ul>

<b>FortiAnalyzer</b>	<ul style="list-style-type: none"> <li>• 5.2.0 and later</li> <li>• 5.0.0 and later</li> <li>• 5.0.0 to 5.0.10</li> </ul>
<b>FortiCache</b>	<ul style="list-style-type: none"> <li>• 3.0.0 to 3.0.8</li> </ul>
<b>FortiClient</b>	<ul style="list-style-type: none"> <li>• 5.2.0 and later</li> <li>• 5.0.4 and later</li> </ul>
<b>FortiMail</b>	<ul style="list-style-type: none"> <li>• 5.2.7</li> <li>• 5.1.5</li> <li>• 5.0.8</li> </ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"> <li>• 2.1.2</li> <li>• 1.4.0 and later</li> <li>• 1.3.0</li> <li>• 1.2.0 and 1.2.3</li> </ul>
<b>FortiSwitch ATCA</b>	<ul style="list-style-type: none"> <li>• 5.0.0 and later</li> <li>• 4.3.0 and later</li> <li>• 4.2.0 and later</li> </ul>
<b>FortiWeb</b>	<ul style="list-style-type: none"> <li>• 5.3.8</li> <li>• 5.2.4</li> <li>• 5.1.4</li> <li>• 5.0.6</li> </ul>
<b>Virtualization</b>	<ul style="list-style-type: none"> <li>• Amazon Web Service AMI, Amazon EC2, Amazon EBS</li> <li>• Citrix XenServer 6.2</li> <li>• Linux KVM Redhat 6.5</li> <li>• Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2</li> <li>• OpenSource XenServer 4.2.5</li> </ul> <p><b>VMware</b></p> <ul style="list-style-type: none"> <li>• ESX versions 4.0 and 4.1</li> <li>• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0</li> </ul>



To confirm that a device model or firmware version is supported by current firmware version running on FortiManager, run the following CLI command:  
`diagnose dvm supported-platforms list`



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

## Feature support

The following table lists FortiManager feature support for managed platforms.

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

## Language support

The following table lists FortiManager language support information.

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

Language	GUI	Reports	Documentation
Spanish		✓	

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

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

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

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

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 5.2.7.

**Supported FortiGate models**

Model	Firmware Version
<p><b>FortiGate:</b> FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B</p> <p><b>FortiGate 5000 Series:</b> FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C</p> <p><b>FortiGate DC:</b> FG-80C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3950B-DC, FG-3951B-DC</p> <p><b>FortiGate Low Encryption:</b> FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p> <p><b>FortiWiFi:</b> FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p><b>FortiGate Rugged:</b> FGR-60D, FGR-100C</p> <p><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p><b>FortiSwitch:</b> FCT-5902D, FS-5203B</p>	5.2

Model	Firmware Version
<p><b>FortiGate:</b> FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FGT-3000D</p> <p><b>FortiGate 5000 Series:</b> FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C</p> <p><b>FortiGate DC:</b> FG-80C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC</p> <p><b>FortiGate Low Encryption:</b> FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p> <p><b>FortiWiFi:</b> FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FG-70D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p><b>FortiGate Rugged:</b> FGR-60D, FGR-90D, FGR-100C</p> <p><b>FortiGateVoice:</b> FGV-40D2, FGV-70D4</p> <p><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p><b>FortiSwitch:</b> FS-5203B, FCT-5903C, FCT-5913</p>	5.0

Model	Firmware Version
<p><b>FortiGate:</b> FG-20C, FG-20C-ADSL-A, FG-30B, FG-40C, FG-50B, FG-51B, FG-60B, FG-60C, FG-60C-POE, FG-60C-SFP, FG-80C, FG-80CM, FG-82C, FG-100A, FG-100D, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-311B, FG-400A, FG-500A, FG-600C, FG-620B, FG-621B, FG-800, FG-800C, FG-800F, FG-1000A, FG-1000AFA2, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B</p> <p><b>FortiGate 5000 Series:</b> 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</p> <p><b>FortiGate DC:</b> 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</p> <p><b>FortiGate Low Encryption:</b> FG-20C-LENC, FG-40C-LENC, FG-50B-LENC, FG-51B-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000A-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC</p> <p><b>FortiWiFi:</b> 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</p> <p><b>FortiGate Rugged:</b> FGR-100C</p> <p><b>FortiGate One:</b> FG-ONE</p> <p><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-XEN, FG-VMX</p> <p><b>FortiSwitch:</b> FS-5203B</p>	4.3

### Supported FortiCarrier models

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

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

### Supported FortiAnalyzer models

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

### Supported FortiMail models

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

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

### Supported FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	2.0
<b>FortiSandbox VM:</b> FSA-VM	1.4
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	1.3
	1.2

### Supported FortiSwitch ATCA models

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

### Supported FortiWeb models

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

**Supported FortiCache models**

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D	3.0 and later
<b>FortiCache VM:</b> FCH-VM64	

## Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.2.7.

### Compatibility issues with FortiOS 5.2.7

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

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

### Compatibility issues with FortiOS 5.2.3

The following table lists interoperability issues that have been identified with FortiManager version 5.2.7 and FortiOS version 5.2.3.

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

### Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.2.7 and FortiOS version 5.2.1.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263896	If it contains the certificate: <code>Fortinet_CA_SSLProxy</code> or <code>Fortinet_SSLProxy</code> , <code>retrieve</code> may not work as expected.

## Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.7 and FortiOS version 5.2.0.

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

## Compatibility issues with FortiOS 5.0.5

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

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

## Compatibility issues with FortiOS 5.0.4

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.7 and FortiOS version 5.0.4.

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

---

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

## Resolved Issues

The following issues have been fixed in 5.2.7. For inquiries about a particular bug, please contact [Customer Service & Support](#).

### Device Manager

Bug ID	Description
365412	Due to memory leaks, FortiManager may be unable to install too many devices or install a large policy package.
294021	SSL-VPN may not list all the available portals when some portals have been mapped by other FortiGate devices or VDOMs. Workaround: Use CLI to copy the missing portals from ADOMs to the database of the targeted FortiGate device.

### Revision History

Bug ID	Description
287632	Install fails with the default SSL VPN self-sign certificate.
305369	Install device changes may fail on the dh-params and upload-option settings.

### Services

Bug ID	Description
365743	FortiManager may not be able to provide update services to FortiGate HA cluster.

## Known Issues

The following issues have been identified in 5.2.7. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

### AP Management

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

### Services

Bug ID	Description
364406	FortiGuard server may run out of memory and crash.

### System Settings

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

## FortiGuard Distribution Servers (FDS)

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

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

## FortiGuard Center update support

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

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	<ul style="list-style-type: none"> <li>• 5.0.0 and later</li> <li>• 5.2.0 and later</li> </ul>	✓		✓	
FortiClient (Windows)	<ul style="list-style-type: none"> <li>• 4.3.0 and later</li> </ul>	✓			
FortiClient (Windows)	<ul style="list-style-type: none"> <li>• 4.2.0 and later</li> </ul>	✓	✓		✓
FortiClient (Mac OS X)	<ul style="list-style-type: none"> <li>• 5.0.1 and later</li> <li>• 5.2.0 and later</li> </ul>	✓		✓	
FortiMail	<ul style="list-style-type: none"> <li>• 4.2.0 and later</li> <li>• 4.3.0 and later</li> <li>• 5.0.0 and later</li> <li>• 5.1.0 and later</li> <li>• 5.2.0 and later</li> </ul>	✓	✓		
FortiSandbox	<ul style="list-style-type: none"> <li>• 1.2.0, 1.2.3</li> <li>• 1.3.0</li> <li>• 1.4.0 and later</li> </ul>	✓			
FortiWeb	<ul style="list-style-type: none"> <li>• 5.0.6</li> <li>• 5.1.4</li> <li>• 5.2.0 and later</li> <li>• 5.3.0</li> </ul>	✓			



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
```

---



High Performance Network Security



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.