



FortiManager Release Notes

VERSION 5.0.11

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



June 18, 2015

FortiManager 5.0.11 Release Notes

02-5011-278522-20150618

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported models	6
What's new in FortiManager version 5.0.11	6
Special Notices	7
SSLv3 on FortiManager-VM64-AWS	7
Monitor upgrade process	7
ADOM upgrade	7
CLI commands for configuring dynamic objects	7
FortiManager VM	8
Unregistered device table	9
FortiAnalyzer feature set	9
FortiGate firmware upgrade	9
System time on FortiManager VM (VMware)	10
Memory requirement for FortiManager VM64 (Hyper-V)	10
ADOM for FortiCarrier	10
FortiOS version 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 version 4.2 devices	12
Endpoint management	12
FortiManager VM license check	12
Multi-language display support	12
New hard disk drive partition layout	12
Importing a FortiManager generated policy	13
Importing profile group and RADIUS dynamic start server	13
Push update in bi-directional static NAT	13
FortiOS 5.2.3 Support	13
Upgrade Information	14
Upgrading from FortiManager version 5.0.6 or later	14
Upgrading from FortiManager version 5.0.5 or earlier	14
Downgrading to previous firmware versions	14
FortiManager VM firmware	15
Firmware image checksums	15

SNMP MIB Files	16
Product Integration and Support	17
FortiManager version 5.0.11 support	17
Feature support	18
Language support	19
Supported models	20
Compatibility with FortiOS Versions	29
Resolved Issues	31
Known Issues	35
Appendix A: FortiGuard	36
FortiGuard Distribution Servers (FDS) and services	36
FortiGuard Center update support	36

Change Log

Date	Change Description
2015-05-25	Initial release.
2015-06-09	Removed FG-1000D and FG-1200D from the v5.0 Supported Device Table.
2015-06-16	Removed FG-3810D and FG-3700DX for v5.2 from the Supported Models List. Removed FG-3200D, FG-70D-POE, FGV-40D2, and FGV-70D4 for v5.0 from the Supported Models List. Added 281040 and 281319 under "Other" section in Known Issues List. Added 267452 under "Other" section in Resolved Issues List.
2015-06-18	Updated FortiOS support from 5.0.4 to 5.0.11 to 5.0.4 to 5.0.12 in the Product Integration Chapter.

Introduction

This document provides the following information for FortiManager version 5.0.11 build 0377:

- [Supported models](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Compatibility with FortiOS Versions](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Appendix A: FortiGuard](#)

Please review all sections in this document prior to upgrading your device. For information on upgrading your device, see the *FortiManager Upgrade Guide*.

Supported models

FortiManager version 5.0.11 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-3900E, FMG-4000E, FMG-5001A.
FortiManager VM	FMG-VM32, FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMG-VM64-KVM, FMG-VM64-XEN

What's new in FortiManager version 5.0.11

The following is a list of new features and enhancements in FortiManager version 5.0.11:

- FortiExtender support

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiManager version 5.0.11.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-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
```

Monitor upgrade process

When upgrading to FortiManager version 5.0.7 or later, FortiManager consolidates dynamic objects from all managing devices to the ADOM database. As a result, the upgrade process takes longer than previous patch releases. The time to complete the upgrade process depends on the number of managed devices and dynamic objects. Please monitor the upgrade progress from the console port. FortiManager prompts the following outputs when consolidating dynamic objects:

```
Upgrading device dynamic objects to Adom DB ...
Upgrading device dynamic objects for 11416/3
Upgrading device dynamic objects for 11416/3 succeeded
Upgrading device dynamic objects for 12614/3
Upgrading device dynamic objects for 12614/3 succeeded
Upgrading device dynamic objects for 12843/3
Upgrading device dynamic objects for 12843/3 succeeded
Upgrading device dynamic objects for 12852/3
...
```

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.

CLI commands for configuring dynamic objects

In FortiManager version 5.0.7 and later, 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.

Unregistered device table

In FortiManager version 5.0.4 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 version 5.0.5 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.

FortiAnalyzer feature set

In FortiManager version 5.0.5 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 FortiManager version 5.0.7 and later 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 (VMware)

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 (Hyper-V)

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 version 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 or the managing FortiManager for update services. If a FortiGate is required to retrieve updates from a specific FortiManager or FortiGuard server, please use port address translation (PAT) to redirect update traffic to the proper IP address and port.



This is applicable to FortiOS version 5.0 and 4.3 devices only. FortiOS version 5.2 has a different behavior..

The following table lists the ports used by FortiGuard Services.

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.

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 version 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, 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 5.0.1 and later have restrictions on supporting a FortiGate device's multi-language display.

New hard disk drive partition layout

FortiManager version 5.0.0 introduced a new hard disk drive partition layout which is required for optimal usage and performance. Following an upgrade to version 5.0.0 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 FDN 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
```

FortiOS 5.2.3 Support

FortiGate units running FortiOS 5.2.3 managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs or after a factory reset of the FortiGate Unit even after a retrieve and re-import policy.

Upgrade Information



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

Upgrading from FortiManager version 5.0.6 or later

FortiManager version 5.0.11 supports upgrading from version 5.0.6 or later.

FortiManager 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.



If your FMG-400B is running 5.0.6, it is required to use an interim step. You **MUST** upgrade to version 5.0.7 before upgrading to 5.0.11. For more information see the *FortiManager 5.0.7 Release Notes*. The upgrade path looks like this:
5.0.5 or earlier > 5.0.6 > 5.0.7 > 5.0.11

Upgrading from FortiManager version 5.0.5 or earlier

In order to accommodate the re-sizing of the flash partition, you **MUST** upgrade to version 5.0.6 first.



Please upgrade your FMG-5001A via the Web-based Manager or command line interface. Upgrade via TFTP from BIOS is not supported for this model.

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 Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Linux KVM

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

Microsoft Hyper-V Server

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

VMware ESX/ESXi

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



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://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>. To verify the integrity of the download, select the *Checksum* link next to the

HTTPS download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

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 5.00 file folder.

Product Integration and Support

FortiManager version 5.0.11 support

The following tables lists FortiManager version 5.0.11 product integration and support information.

Web Browser	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 38 • Google Chrome version 42 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 5.2.3 • 5.2.2 • 5.2.1 FortiManager version 5.0.11 is fully tested as compatible with FortiOS/FortiOS Carrier version 5.2.1, with some minor interoperability issues. • 5.2.0 FortiManager version 5.0.11 is fully tested as compatible with FortiOS/FortiOS Carrier version 5.2.0, with some minor interoperability issues. • 5.0.4 to 5.0.12 FortiManager version 5.0.11 is fully tested as compatible with FortiOS/FortiOS Carrier version 5.0.4 to 5.0.12, with some minor interoperability issues. • 4.3.2 and later • 4.2.0 and later
FortiGate Voice	• 5.0.0
FortiAnalyzer	• 5.2.0 to 5.2.1 • 5.0.0 and later
FortiCache	• 3.0.0 to 3.0.2
FortiClient	• 5.2.0 and later • 5.0.4 and later

FortiMail	• 5.2.0 to 5.2.3 • 5.1.3 to 5.1.4 • 5.0.6 to 5.0.7
FortiSandbox	• 2.0.2 • 1.4.0 and later • 1.3.0 • 1.2.0 and later
FortiSwitch ATCA	• 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.3.0 to 5.3.5 • 5.2.3 to 5.2.4 • 5.1.4 • 5.0.6
Syslog	• Standard syslog
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix Xen Server 6.2 • Linux KVM Redhat 6.5 • Microsoft Hyper-V Server 2008 R2 and 2012 • OpenSource XenServer 4.2.5 VMware • ESX versions 4.0 and 4.1 • ESXI versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiAnalyzer				
FortiCache			✓	✓
FortiCarrier	✓	✓	✓	✓
FortiClient		✓		✓

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiMail		✓	✓	✓
FortiSandbox	✓	✓		✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

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

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

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

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

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

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

Supported models

The following tables list which FortiGate, FortiGateVoice, FortiCarrier, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager device running FortiManager version 5.0.11.

Supported FortiGate models

Model	Firmware Version
FortiGate FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-POE, FG-60D-3G4G-VZW, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1000D, FG-1200D, 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-5001D, FG-5101C	5.2
FortiGate DC FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-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, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC	
FortiWiFi FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE. FWF-92	
FortiGate Rugged FGR-60D, FGR-100C	
FortiGate VM FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN	
FortiSwitch FS-5203B	

Model	Firmware Version
FortiGate FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3000D, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5001D, FG-5101C	5.0
FortiGate DC FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC	
FortiWiFi FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-60D, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D	
FortiGate Rugged FGR-60D, FGR-90D, FGR-100C	
FortiGate VM FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN	
FortiSwitch FS-5203B	

Model	Firmware Version
FortiGate	4.3
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, FG- 5001, FG-5001A, FG-5001B, FG-5001C, FG-5001FA2, FG-5002A, FG- 5002FB2, FG-5005FA2, FG-5101C	
FortiGate DC	
FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-600C-DC, FG- 621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG- 3140B-DC, FG-3240C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption	
FG-20C-LENC, FG-40C-LENC, FG-50B-LENC, FG-51B-LENC, FG-60C- LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000A-LENC, FG- 1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG- 3810A-LENC, FG-3950B-LENC, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001FA2-LENC, FG-5001A-SW-LENC, FG-5002A-LENC	
FortiWiFi	
FWF-20C, FWF-20C-ADSL-A, FWF-30B, FWF-40C, FWF-50B, FWF-60B, FWF-60C, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF- 80CM, FWF-81CM	
FortiGate Rugged	
FGR-100C	
FortiGate One	
FG-ONE	
FortiGate VM	
FG-VM, FG-VM64, FG-VM64-XEN	
FortiSwitch	
FS-5203B	

Model	Firmware Version
FortiGate FG-30B, FG-50B, FG-51B, FG-60B, FG-60C, FG-80C, FG-80CM, 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-311B, FG-400A, FG-500A, FG-620B, FG-621B, FG-800, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, 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-5002A, FG-5002FB2, FG-5005FA2	4.2
FortiGate DC FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-621B-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption FG-50B-LENC, FG-51B-LENC, FG-60C-LENC, FG-80C-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-620B-LENC, FG-1000A-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001FA2-LENC, FG-5001A-SW-LENC, FG-5002A-LENC	
FortiWiFi FWF-30B, FWF-50B, FWF-60B, FG-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60CM, FWF-80CM, FWF-81CM,	
FortiGate One FG-ONE	
FortiGate VM FG-VM	

Supported FortiGateVoice models

Model	Firmware Version
FortiGateVoice	5.0

Supported FortiCarrier models

Model	Firmware Version
FortiCarrier FCR-3240C, FCR-3600C, FCR-3700D, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C	5.2
FortiCarrier DC FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3910B-DC, FCR-3950B-DC	
FortiCarrier Low Encryption FCR-5001A-DW-LENC	
FortiCarrier VM FCR-VM, FCR-VM64	
FortiCarrier FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	5.0
FortiCarrier DC FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC	
FortiCarrier Low Encryption FCR-5001A-DW-LENC	
FortiCarrier VM FCR-VM, FCR-VM64	
FortiCarrier FG-60B, FG-80C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	4.3
FortiCarrier DC FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC	
FortiCarrier Low Encryption FCR-5001A-DW-LENC	

Model	Firmware Version
FortiCarrier	4.2
FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	
FortiCarrier DC	
FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC	
FortiCarrier Low Encryption	
FCR-5001A-DW-LENC	

Supported FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer	5.2
FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B	
FortiAnalyzer VM	
FAZ-VM, FAZ-VM64	
FortiAnalyzer	5.0
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-3900E, FAZ-4000A, FAZ-4000B	
FortiAnalyzer VM	
FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV, FAZ-VM63-KVM, FAZ-VM64-XEN	
FortiAnalyzer	4.3 4.2
FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A	

Supported FortiCache models

Model	Firmware Version
FortiCache	3.0
FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D	
FortiCache VM	
FCH-VM64	

Supported FortiMail models

Model	Firmware Version
FortiMail	5.2
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B	5.1
FortiMail VM	
FE-VM64	
FortiMail	5.0
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B	
FortiMail VM	
FE-VM64	

Supported FortiSandbox models

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

Supported FortiSwitch ATCA models

Model	Firmware Version
FortiController	5.2
FTCL-5902D	

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

Supported FortiWeb models

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

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager version 5.0.11.

Compatibility issues with FortiOS version 5.2.3

Bug ID	Description
271059	FortiGate units running FortiOS 5.2.3 managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs or after a factory reset of the FortiGate Unit even after a retrieve and re-import policy. The issue will be addressed in FortiManager 5.2.2 and later releases.

Compatibility issues with FortiOS version 5.2.1

Bug ID	Description
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 version 5.2.0

Bug ID	Description
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 .
0246153	Remove AIM, ICQ, MSN, and Yahoo selections from the DLP sensor.

Compatibility issues with FortiOS version 5.0.5

Bug ID	Description
0230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS version 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS version 5.0.6.

Compatibility issues with FortiOS version 5.0.4

Bug ID	Description
0226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS version 5.0.5.
0226078	When the password length is increased to 128 characters, the installation fails.

Bug ID	Description
0226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS version 5.0.5.
0226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS version 5.0.5.
0226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS version 5.0.5.
0226236	The set dedicated-management-cpu enable and set user-anonymize enable CLI commands fail on device install. These commands were added in FortiOS version 5.0.5.
0230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS version 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS version 5.0.6.

Resolved Issues

The following issues have been fixed in FortiManager version 5.0.11. For inquiries about a particular bug, please contact [Customer Service & Support](#).

GUI

Bug ID	Description
215424	FortiManager may not be able to reserve an IP address for a MAC address in the DHCP server.
218286	When the Workflow mode is enabled, the Database Configuration may display changes that have not been saved.
219791	The FortiManager may not support the new FortiController Trunk interface.
259988	In the VDOM properties, you may not be able to set Guarantee Resources.
266073	When changing FortiGate-60D or FortiWiFi-60D Interface mode from Internal to Switch, the Internal interface may disappear.
267272	Following a FortiGate failover, the FortiGate HA Cluster Member status may not update in the GUI.
267964	In the Unregistered Device List, FortiGate Cluster Members may appear as Logging Only Device.

Global ADOM

Bug ID	Description
268222	IPS signatures may be missing.

Other

Bug ID	Description
261564	After an ADOM upgrade, the policy <code>tcp-reset</code> setting may be reset.
264465	After an ADOM upgrade from v5.0 to v5.2, the policy packages and objects may disappear.
266330	The ADOM list max value may not be the same as the max number of ADOMs supported by a platform.
269623	The FortiManager may not backup all settings via SCP.

Bug ID	Description
267452	Fixes resolve issues related to the CVE-2015-0235 “GHOST” vulnerability.

Policy & Objects

Bug ID	Description
256261	FortiManager will always install <code>profile-protocol-options</code> on a policy with an IPS sensor.
261689	In some cases, users may not be able to delete firewall VIP objects even when they are not in use.
262208	<code>Used</code> may not only return <i>No Records Found</i> .
263973	Due to missing User DN and Password fields, users may not be able to map dynamic regular-type LDAP servers.
264536	Static URL Filter with Wildcard may not be supported.
265574	Due to reach the object limit of 1000, FortiManager may not be able to push Global Policy to the FortiGate.
267164	In Workflow mode, Local Certificate Mappings may not be saved.
268402	When adding a new element in the DNS Database, with a dash (–) symbol, the <i>Runtime error 12: illegal name</i> message may appear.
269768	When creating a new dynamic local certificate with ADOM v5.2, the FortiManager may not list Local Certificates for Mapping.
271642	If <code>Used</code> contains two dynamic firewall addresses mapped to two separate devices, it may not work on an address group.
271732	Inconsistent SSL VPN Portal options may occur between FortiManager and FortiGate v4.3.
272120	The Virtual IP Pool ARP interface may not be able to use a zone with a name longer than 15 characters.
272429	In some cases, users may not be able to install changes to a firewall address object created with the IP address: 255.255.255.255.
272958	If a Firewall Object is created with a + in the name, users may not be able to edit it.
273543	FortiManager may not be able to change a policy from WAN Optimization Active to Passive and visa versa.

Bug ID	Description
273340	When copying and pasting multiple policies at once, the FortiManager may use high system resources.
277062	When the password is reset within ADOM v4.3, users may be removed from the User Group.

Revision History

Bug ID	Description
162871	FortiManager may send incomplete commands to the FortiGate's SSID settings, and may report a successful installation.
258538	After upgrade, installation may not complete on System Replacement messages.
269702	When pushing Threat Weight template-related-configurations, installation may not complete on non-root VDOM.
269727	Installation may not work on Local Rating Configuration with category 24.
270147	Due to invalid real-time log upload setting, the policy installation may not work as expected.
272606	Verification may not work after modifying FortiAnalyzer log settings.
274882	Due to a conflict between <code>/x</code> and <code>255.x.xx</code> netmask notation, installation may not work.
279848	FortiManager may not be able to install <code>ssl-cipher-suites</code> setting for VIP addresses.

Script

Bug ID	Description
265674	When adding multiple management IPs in TP mode, the CLI script may not work.

Services

Bug ID	Description
249397	The entry on updated time may be inconsistent with the update history.
265739	When the connection between a FortiManager and FDS is lost, the FortiGate-VM license validation may become unstable.

System Settings

Bug ID	Description
256864	When a device is Auto-updated and Imported, the Event Log entries may become unclear or they may be missing.
271862	During a restart or shutdown of a FortiGate device, the FortiManager might not generate a log.

VPN Console

Bug ID	Description
211154	Between Start and Mesh topologies, FortiManager may have inconsistent Automatic Route Behavior with external gateways.
271862	FortiManager may show duplicated remote gateway error related to multi-hubs VPN.

Known Issues

The following issues have been identified in FortiManager version 5.0.11. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

GUI

Bug ID	Description
271807	When the FortiGate is in HA Mode, the SNMP Community Host interface might not be recognized.

Policy and Objects

Bug ID	Description
275568	After users submit FortiClient XML Configuration changes, they may not be saved.

Other

Bug ID	Description
274415	The SNMP Trap OID, 1.3.6.1.4.1.12356.100.1.3.0.409 may not be in the MIB file.
281040	FortiManager may be unable to add FortiGate-1000D and FortiGate-1200D.
281319	FortiManager may not currently support: FG-3810D, FG-3810D-DC, FG-3700DX, FG-3200D, FG-70D-POE, FGV-40D2, and FGV-70D4.

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 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.

FortiGuard Center update support

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	• 5.0 • 5.2	✓		✓	
FortiClient (Windows)	• 4.3	✓			
FortiClient (Windows)	• 4.2	✓	✓		✓
FortiClient (Mac OS X)	• 5.0	✓		✓	
FortiMail	• 4.2 • 4.3 • 5.0 • 5.1 • 5.2	✓	✓		

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiSandbox	• 1.2	✓			
	• 1.3				
	• 1.4				
	• 2.0				
FortiWeb	• 5.0	✓			
	• 5.1				
	• 5.2				
	• 5.3				



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
```



Copyright© 2015 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.