FortiManager Release Notes

VERSION 5.2.4

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

November 02, 2015

FortiManager 5.2.4 Release Notes

02-524-292520-20151102

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-09-24	Initial release.
2015-10-07	Added bugs 287811 and 275919 to Resolved Issues List.
2015-10-27	Added 248166 to Known Issues List.
2015-10-28	Added FG-600D to 5.2 Supported FortiGate Models. Added FG-900D to 5.0 Supported FortiGate Models.
2015-11-02	Updated 248166 and added to Special Notices.
2016-02-19	Added FortiOS/FortiOS Carrier 5.2.5 and 5.2.6 to FortiManager 5.2.4 support.
2016-02-24	Updated language support

Introduction

This document provides the following information for FortiManager 5.2.4 build 738:

- Supported models
- Special Notices
- Upgrade Information
- Product Integration and Support
- Compatibility with FortiOS Versions
- Resolved Issues
- Known Issues
- FortiGuard Distribution Servers (FDS)

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

Supported models

FortiManager version 5.2.4 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM32, FMG-VM64, 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 5.2.4.

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. For FortiManager units that are upgraded from a previous release, all multicast policies must be imported into the ADOM database or reconfigured manually. 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 t1sv1
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 5.2.4, 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
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 from FortiManager 5.2.0 to 5.2.4

FortiManager 5.2.4 supports upgrade from 5.2.0 or later to 5.2.4.

Upgrading from FortiManager 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.

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

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the 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-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://wwwfortinet.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 5.2.4 support

The following table lists 5.2.4 product integration and support information:

Web Browsers	• Microsoft Internet Explorer™ 11.0 • Mozilla Firefox version 40 • Google Chrome version 45 Other web browsers may function correctly, but are not supported by Fortinet. Please make sure your computer's screen resolution is set to at least 1280x1024. Otherwise, web pages may not be displayed properly.
FortiOS/FortiOS Carrier	• 5.2.6 FortiManager 5.2.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see "Compatibility with FortiOS Versions" on page 27. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.2.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 27. • 5.2.0 FortiManager 5.2.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility with FortiOS Versions on page 27. • 5.0.4 to 5.0.12 FortiManager 5.2.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.04 to 5.0.12, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 27. • 4.3.2 to 4.3.18

FortiAnalyzer	• 5.2.0 and later • 5.0.0 and later • 5.0.0 to 5.0.10
FortiCache	• 3.0.0 to 3.0.5
FortiClient	• 5.2.0 and later • 5.0.4 and later
FortiMail	• 5.2.4 • 5.1.5 • 5.0.8
FortiSandbox	• 2.1.0 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.3.7 • 5.2.4 • 5.1.4 • 5.0.6
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 6.2 • Linux KVM Redhat 6.5 • Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2 • 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

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)	✓	✓	

Language	GUI	Reports	Documentation
French		✓	
Japanese	✓	✓	
Korean	✓	✓	
Portuguese		✓	
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 5.2.4.

Supported FortiGate models

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-300C-DC, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-1000C,FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3000D-DC, FG-3016B, FG-3040B, FG-3100D-DC,FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3800D, FG-3810A, FG-3810D, FG-3810D-DC, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM, FG-VM64,FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.2

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-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-300C-DC, 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-3000D, FG-3000D-DC, FG-3016B, FG-3040B, FG-3100D-DC, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92 **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiGate Voice**: FGV-40D2, FGV-70D4 **FortiSwitch:** FS-5203B, FCT-5903C, FCT-5913C	5.0

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30B, FG-40C, FG-50B, FG-51B, FG-60B, FG-60C, FG-60C-POE, FG-60C-SFP, FG-80C, FG-80CM, FG-82C, FG-100A, FG-100D, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C,FG-300C-DC, 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 **FortiGate 5000 Series:** FG-5001, FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001FA2, FG-5001FA2-LENC, FG-5002A, FG-5002A-LENC, FG-5002FB2, FG-5005FA2, FG-5005FA2-2G, FG-5005FA2-4G, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-600C-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-50B-LENC, FG-51B-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30B, FWF-40C, FWF-50B, FWF-60B, FWF-60C, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM **FortiGate Rugged:** FGR-100C **FortiGate One:** FG-ONE **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-XEN **FortiSwitch:** FS-5203B	4.3

Supported FortiCarrier models

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

Supported FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-HV	5.2

Model	Firmware Version
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV	5.0

Supported FortiMail models

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

Supported FortiSandbox models

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

Supported FortiSwitch ATCA models

Model	Firmware Version
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

Supported FortiWeb models

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

Supported FortiCache models

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

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.2.4.

Compatibility issues with FortiOS 5.2.6

The following table lists interoperability issues that have been identified with FortiManager version 5.2.4 and FortiOS 5.2.6.

Bug ID	Description
308294	1) New default wtp-profile settings on FOS 5.2.6 cause verification errors during installation. 2) FortiManager only supports 10,000 firewall addresses while FortiOS 5.2.6 supports 20,000 firewall addresses.

Compatibility issues with FortiOS 5.2.3

The following table lists interoperability issues that have been identified with FortiManager version 5.2.4 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 `Retrieve` after the install.

Compatibility issues with FortiOS 5.2.2

The following table lists interoperability issues that have been identified with FortiManager version 5.2.4 and FortiOS version 5.2.2.

Bug ID	Description
287632	Install fails with the default SSL VPN self-sign certificate.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.2.4 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: `Fortinet_CA_SSLProxy` or `Fortinet_SSLProxy`, `retrieve` 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 5.2.4 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 5.2.4 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 `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
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 5.2.4. For inquires about a particular bug, please contact Customer Service & Support.

GUI

Bug ID	Description
278164	Interface page cannot load because of the missing VDOM setting in the `mgmt` interface.
284080 287885	During the policy package import process, FortiManager cannot *View Detail* or *Download Conflict File*.
288184	When the install wizard is canceled, the task stops working in the Task Monitor.
268793	FortiManager reports an error when changing resource usage on Firewall Addresses.
278968	FortiManager cannot add descriptions to MAC address list under a DHCP server.
284806	*Search Group* function does not work in *Add Device* context.
289515	FortiManager should not allow users to create a static route with a distance of `0`.
290104	FortiManager prompts *Runtime error 131* when creating a VLAN with a DHCP server configuration.
290255	When adding an interface to a WAN Link Load Balancing interface, *Measure Link Quality* is selected and it cannot be changed.
290999	FortiManager cannot configure the DHCP Relay on Hardware Switch interface when set to *Internal*.

Global ADOM

Bug ID	Description
288087	After upgrading, Global Policy changes are not pushed to the ADOM level.
277330	Assigning a global policy package should trigger ADOM policy packages to show a modified status.

Other

Bug ID	Description
253961	Display the system uptime in a readable format instead of the Linux Epoch format.
284528	JSON API cannot obtain the Global ADOM's Policy Package Exclusion List.
288160	FortiManager cannot install a policy via the `installConfig SOAP XML` request; it returns the *no write permission* error message.
284677	Policy Package Status is changed to *Modified* after upgrade.
290754	Running two instances of the SOAP XML `runScript` concurrently against two different ADOMS will causes one of the devices to stop working.
292007	FortiManager records incorrect user name for *Configuration Change Event* in Event logs.

Policy and Objects

Bug ID	Description
256261	FortiManager will always install `profile-protocol-options` on a policy with an IPS sensor.
279052	When editing an address group and applying a filter with a specific IP, FortiManager should not include members that are already part of the group.

Bug ID	Description
285788	Installation fails if CA certificate from ADOM database already exists on FortiGate with a different name.
286119	Dynamic Mapping for a Global Address Object is not installed into the FortiGate device.
288091	When a Per-Device Mapping is configured on a Load Balance Object, FortiManager shows the *Loading Aborted* error on the Virtual IP page.
288226	If a FortiGate device is removed with Dynamic Mapping configured on the objects, some object pages display the *Loading Aborted* error message.
288655	The Policy interface selection drop down list does not show zones or interfaces.
291230	By default, the Implicit Policy should be *On* in the Display Options for policy package display.
290213	Editing URL Filter type should only save the edited entry without keeping the original entry.
290252	FortiManager returns the *Runtime Error 131* when right-clicking to add a `WAN-load-balance` interface.
233189	`IPSec phase2` selector does not support IPv6.
238233	Web Proxy Forwarding Server drop down list *Create New* does not work as expected.
276806	Scheduled installs from `TACAS+ wildcard` user does not work as expected.
283950	*Policy Search* feature does not work correctly with collapsed sections.
285586	Load balance VIP option *Preserve Client IP* is not available without `HTTP(S) Multiplexing` enabled.
287248	After a global policy package is assigned, the global icon should be displayed next to related policy packages.
288704	WAN optimization cannot be enabled via FortiManager.
291043	Restricted admin pushing an object change results in a policy package to be in conflict.

Bug ID	Description
288754	When Per-Device Mapping is configured on a Load Balance, the FortiManager is not able to install Real Server Settings to the FortiGate.
290986	FortiManager prompts runtime error while configuring address groups with URL objects.

Revision History

Bug ID	Description
286392	FortiManager resets the IPS block duration if *Quarantine* is disabled.
286686	FortiManager should use `set auth radius` when the security mode requires RADIUS.
287879	FortiManager prompts install verification failure after upgrading to 5.2.3.
287881	Incorrect Revision History entry is highlighted.
287882	Nested dynamic address group changes are not installed.
282097	FortiManager does not install `security-groups` to Captive Portal.

Script

Bug ID	Description
286111	TCL Script stops working if the FortiGate SSH Port Number is not 22.
290005	If the user changes any admin settings, `rpc-permit` is reset to `None`.

Services

Bug ID	Description
277389	FortiManager stops working when service access `fclupdates` is enabled on a port number other than 80.
287811	`um_db_service` consumes high IO resource.

System Settings

Bug ID	Description
285956	A device level install is incorrectly logged as an Install Package in the Task Monitor.
286889	When the Global Database is upgraded from 5.0 to 5.2, it returns the error: *fail (errno=-1):unknown*.

VPN Console

Bug ID	Description
289900	The VPN Console should not generate a Static Route on the hub for its own protected subnet.

Known Issues

The following issues have been identified in 5.2.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

GUI

Bug ID	Description
289963	When a user changes anything on an IPSec interface that is bonded to a `npu-link`, FortiManager tries to change its address from `0.0.0.0/0.0.0.0` to `0.0.0.0/255.255.255.255`.
292218	FortiManager may return *Runtime error 89: duplicate ip in the list* when creating a DHCP relay.
275919	FortiManager cannot add a FortiGate if an interface sets `dmgmt-vdom` as the designated VDOM. Workaround: Please specify another supported VDOM instead of `dmgmt-vdom`.

Other

Bug ID	Description
292138	RADIUS wildcard user cannot login via JSON API.

Revision History

Bug ID	Description
292459	SSID configured with security mode with captive portal and portal type with *Disclaimer Only* does not get pushed to the FortiGate device.

System Settings

Bug ID	Description

284439	FortiManager may generate many *https connection* logs for web GUI accesses.
	
	Workaround: Leave the log severity level at *information*. Alternatively, if *debug* level is desired, apply filter to set logging on *system* to *disable*:
	`config system locallog disk filter`
	`set system disable`
	`end`

VM

Bug ID	Description
248166	A Hyper-V FAZ-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel based PC.

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)	• 5.0.0 and later • 5.2.0 and later				
FortiClient (Windows)	• 4.3.0 and later				
FortiClient (Windows)	• 4.2.0 and later				
FortiClient (Mac OS X)	• 5.0.1 and later • 5.2.0 and later				
FortiMail	• 4.2.0 and later • 4.3.0 and later • 5.0.0 and later • 5.1.0 and later • 5.2.0 and later				
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later				

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiWeb	• 5.0.6 • 5.1.4 • 5.2.0 and later • 5.3.0				

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

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