FORTINET®

High Performance Network Security

FortiManager Release Notes

VERSION 5.2.2

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

October 1, 2015

FortiManager 5.2.2 Release Notes

02-522-0270205-20151001

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-04-15	Initial release.
2015-04-16	Added additional supported models to the Product Integration and Support Chapter.
2015-04-17	Added bug 275350 to Known Issues list.
2015-05-01	Added VM Partition information to the Upgrade Information chapter. Added Multicast Policy Support, ADOM for FortiGate 4.2 devices, and SSLv3 information to Special Notices. Added 277034 to Known Issues List.
2015-06-02	Updated Upgrade Information Chapter.
2015-06-09	Removed FG-1000D and FG-1200D from the v5.0 Supported Device Table.
2015-06-10	Included FortiOS 5.0.11 and 5.0.12 support to Product Integration.
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.
2015-10-01	Added FortiManager-200E to Supported Models.

Introduction

This document provides the following information for FortiManager 5.2.2 build 706:

- Supported models
- What's new in FortiManager 5.2.2
- 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 5.2.2 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-200E, 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.

The following models are released on a special branch based off of FortiManager 5.2.2.

FMG-200E	FMG-200E is released on build 4077.

What's new in FortiManager 5.2.2

The following is a list of new features and enhancements in 5.2.2.

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

- Ability to create Device Group from Task Monitor
- Progress bar on upgrade status display
- LDAP Browse
- Multicast Policy and Objects support at the ADOM level
- FortiExtender support

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.2.2.

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 5.2.2, 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 and 4.3 devices only. FortiOS version 5.2 has a different behavior.

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 and 5.2.1

FortiManager 5.2.2 supports upgrade from 5.2.0 and 5.2.1.

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 5.2.2 support

The following table lists 5.2.2 product integration and support information:

Web Browsers	• Microsoft Internet Explorer 11.0 • Mozilla Firefox version 37 • Google Chrome version 41 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 5.2.2 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions. • 5.2.0 FortiManager 5.2.2 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility with FortiOS Versions. • 5.0.4 to 5.0.12 FortiManager 5.2.2 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. • 4.3.2 to 4.3.18
FortiAnalyzer	• 5.0.0 to 5.0.10
FortiCache	• 3.0.0 to 3.0.3
FortiClient	• 5.2.0 and later • 5.0.4 and later
FortiMail	• 5.2.3 • 5.1.5 • 5.0.8

FortiSandbox	• 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	• 5.3.5 • 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 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

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.

Feature support per platform

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✔	✔	✔	✔

Feature support per platform

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

Language support

The following table lists FortiManager language support information.

Language support

Language	GUI	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, 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 5.2.2.

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-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-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-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-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.2

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-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-1000C, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3140B, 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-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5903C, FCT-5913C	5.0

Supported FortiGate models

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

Supported FortiAnalyzer models

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 5.2.2.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.2.2 and FortiOS version 5.2.1.

Compatibility issues with FortiOS 5.2.1

Bug ID	Description
0262584	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 5.2.2 and FortiOS version 5.2.0.

Compatibility issues with FortiOS 5.2.0

Bug ID	Description
0262584	When creating a VDOM for the first time it fails.
0263949	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.

Compatibility issues FortiOS 5.0.5

Bug ID	Description
0230199	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 5.2.2 and FortiOS version 5.0.4.

Compatibility issues with FortiOS 5.0.4

Bug ID	Description
0226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
0226078	When the password length is increased to 128 characters, the installation fails.
0226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
0226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 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 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 5.0.5.
0230199	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 5.2.2. For inquires about a particular bug, please contact Customer Service & Support.

GUI

Resolved GUI issues

Bug ID	Description
212554	In some cases, a *Loading Aborted* message may appear when connecting to a FortiAP.
2128286	The Database Configuration may display changes that have been save on the workspace.
230663	After importing a web filter profile, with the *equal to all* option selected in the `category-override`, all local categories may be marked as disabled.
249201	The FortiManager may not be able to add more than three trusted hosts for a FortiGate admin user.
252318	The ADOM Revision Storage Limitation may not be enforced on an install.
258985	Due to a conflict, an object may not import and an error message may not be displayed in the GUI.
258997	Increased task list size may not be taken into account.
259988	FortiManager may not be able to set guaranteed resources in the VDOM properties.
262623	FortiManager may not be able to add a NTP server via the GUI.
262908	A trusted host may not be able to be removed on the GUI.
264757	The FortiGate SLBC blade may not be detected. The error message *Connectivity error DUAL Chassis Failover Event* may be displayed.
267964	In the *Unregistered Device List*, the FortiGate cluster member may appear as a *Logging Only* device.
268529	The FortiManager may not be able to configure the OSPF passive-interface list from the GUI.
166752	Users may not be able to update ADOM configurations that were copied over to the device database.
215424	FortiManager may not be able to reserve an IP address for a MAC address in the DHCP server
234400	FortiGate HA status may not refresh promptly in the GUI.

Resolved GUI issues

Bug ID	Description
247713	Device Group's members may not be listed in alphabetical order when editing a group.
259985	The Application Sensor Clone action may not work as expected.
265016	The HA status of managed devices may not be displayed correctly.
265742	The FortiManager may not be able to access the Device Dashboard menu from a device group.
266936	The FortiManager may not be able to accept remote device change when the workflow is enabled.

Global ADOM

Resolved Global ADOM issues

Bug ID	Description
268222	IPS signatures may be missing under the Global ADOM.
263980	Global Policy Package Assignment may not be possible to some policy packages.
268789	When the workspace is enable, users may need to lock the ADOM in order to exclude a policy package from the assignment.

Other

Other resolved issues

Bug ID	Description
241081	In some cases, users may be able to make configuration changes on a FortiManager HA slave unit.
259086	After an upgrade, administrators may not be able to view the Revision History if the device version does not match the ADOM version.
261564	After an ADOM upgrade, the policy `tcp-reset` setting may be reset.
264465	After an ADOM upgrade from v5.0 to v5.2, the policy package and object may disappear.
264944	In the Diagnoses DVM Device List, the FortiManager may show incorrect *Out-of-Sync Configuration Statuses*.
264117	There may be no event log generated for a JSON login or logout.

Other resolved issues

Bug ID	Description
191191	Users may not be able to copy and paste PSK change in Google Chrome or Internet Explorer.
269623	FortiManager may not backup all settings via SCP.
270838	Security improvements may not be implemented to prevent TLS FREAK attack: CVE-2015-0204
272141	SSL improvements to resolve vulnerabilities: CVE-2015-0209 and CVE-2015-0288.
267452	Fixes resolve issues related to the CVE-2015-0235 “GHOST” vulnerability.

Policy and Objects

Resolved policy and objects issues

Bug ID	Description
210175	Pre-defined IPS Sensor Signature List may not be automatically updated and may be displayed incorrectly.
237826	Administrators may be unable to easily identify and delete unused ADOM object.
249905	A validation policy may not be implemented after dragging and dropping a server object.
252030	After renaming a firewall address object, the associated policy may not be displayed.
254376	The FortiManager may not be consistent with the Firewall Policy IDs and sequence numbers between the GUI and CLI.
258841	The FortiManager may allow user to create incorrect guest user groups.
259333	SMS Configuration under the User definition may not be able to be edited or removed.
259818	In ADOM v5.0, some of the SSLVPN settings options may have not been removed.
260177	When editing an IPS Sensor, signatures from the extended IPS database may not be available.
261357	When two VIPs have identical external IP and different `srcintf-filter`, a conflict value and copy fail may occur.
261982	When the filter is applied and the column is removed, the funnel may disappear from the column.
262431	In some cases, the FortiManager may not install the `auto-asic-offload` setting.
263952	The `fmgd daemon` may crash when adding a custom IPS signature.

Resolved policy and objects issues

Bug ID	Description
264235	It may be possible to add a URL type address to an address group.
264536	The Static URL Filter with Wildcard may not be supported.
264622	The Installation Preview may render the CLI Configuration with HTML syntaxes.
266334	IPS Signatures may not be accepted.
266700	If the firewall address is `used error` the policy package install may not work.
266850	If there is an error on the VIP `src-filter` setting, the policy package install may not work.
268896	In some cases, the FortiManager may not check for duplicate MACs on the user's device settings before attempting to install.
261689	In some cases, users may not be able to delete firewall VIP object even when they are not in use.
262010	Policies in a policy package with a given status may not be displayed.
263973	Users may not be able to map dynamic regular type LDAP servers due to missing User DN and Password field.
266175	Default mapping for dynamic interface may not be supported.
266711	When working in a locked Policy Package, users may not be able to manage Section Titles.
268402	When adding a new element in the DNS Database with a dash (`-`) symbol, the *Runtime error 12: illegal name* message may appear.
268602	After upgrading ADOM/Global ADOM from v5.0 to v5.2, the Policy Meta Datafields may be missing.
269118	Users may not be able to configure the `nat-source-vip` via WebUI.
269578	When a policy package is locked, the *insert above/below* function may not work.
269768	When creating a new dynamic local certificate with v5.2 ADOM, FortiManager may not list local certificates for mapping.
270534	The first workspace sessions may not be able to attach configuration changes in an Email for workflow administrators.
270484	FortiManager may not be able to store or install `ssl-cipher-suites` for firewall VIP addresses.
271012	In FortiManager, the `diffservcode-rev` CLI parameter may be ignored.
271607	When pushing the configuration to disable FortiGuard logging, installation may not work.

Resolved policy and objects issues

Bug ID	Description
272120	The Virtual IP Pool ARP interface may not be able to use a zone with a name longer than 15 characters.
272413	FortiManager may not be able to add a VIP with Any Source Address.
273543	FortiManager may not able to change policy from WAN Optimization *Active* to *Passive* and visa versa.

Revision History

Resolved revision history issues

Bug ID	Description
162871	The FortiManager may send incomplete commands to the FortiGate's SSID settings, and may report a successful installation.
169110	Configuring a SSL route may require a default gateway value and installation may not work.
258124	The FortiManager may remove `extended-utm-log-enable` on a web filter profile.
261509	When attempting to configure a secondary interface IP, the installation may not work.
263114	The FortiManager may try to push *Set Optimize Antivirus* to unsupported low end devices.
264236	After an AP Profile Configuration change, the installation may not work.
157160	When a new auto-update Revision History is automatically created, it may not become the current Revision History.
270147	Due to invalid real-time log upload setting, the policy installation may not work as expected.

Script

Resolved script issues

Bug ID	Description
250084	Under a specific VDOM, the CLI Script may not support system interface changes.
259442	If any device filter is enabled, the FortiManager may not be able to run the script against a device group.
265674	When adding multiple management IPs in TP mode, CLI script may not work.

Services

Resolved service issues

Bug ID	Description
242443	Within Package Management and Service Status, the list of ADOMs may be in reverse alphabetical order.
265739	FortiGate-VM license validation may be unstable when the connection between FortiManager and FDS is lost.

System Settings

Resolved system settings issues

Bug ID	Description
257223	After a *Retrieve Operation*, the FortiManager may be missing ADOM field name information in the event log.
257224	When a *Revision Name* is manually changed, incorrect information may be logged to the event log.
262799	When *Schedule Update* is enabled, the FortiManager may report connectivity errors to the FortiGuard FDS.
256864	When a device is Auto-updated and Imported, Event Log entries may be unclear or missing.
257162	In Event Log files, unclear FortiGuard remote IP may be displayed.
262998	During a reboot or shutdown of a FortiGate device, the FortiManager may not generate a log.

VPN Console

Resolved VPN console issues

Bug ID	Description
255504	*Error 34* may cause the FortiManager to be unable to swap VPN gateway IP address in Managed Gateway Configurations.
265145	When the Aggressive Mode Dialup VPN has a Dailup Group Peer Type, an incorrect *PSK* may be installed on the Dialup Spoke.

Resolved VPN console issues

Bug ID	Description
211154	Between Start and Mesh topologies, FortiManager may have inconsistent Automatic Route Behaviour with external gateways.
27862	Using the same hub-to-hub- interface in multiple multi-hub VPNs may create a duplicate remote gateway error.

Known Issues

The following issues have been identified in 5.2.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

GUI

Known GUI issues

Bug ID	Description
271286	The FortiManager may not allow users to upload images greater than 6KB in the Replacement Message.
274080	When changing the split-tunneling settings in the IPSec Phase1 for dialup, the FortiManager may prompt and incorrect warning message.
274490	After an edit, the FortiManager may show a different interface summary page.
277034	The FortiManager may set and retain the DHCP Relay Setting in the SSID or switch port.

JSON API

Known JSON API issues

Bug ID	Description
276245	Users may not be able to make changes via JSON APIs if FortiManager is behind a firewall.

Other

Known Other issues

Bug ID	Description
271466	When creating a policy with JSON API, if the action is set as *deny*, the default `logtraffic` may be `utm`.
274415	The `1.3.6.1.4.1.12356.100.1.3.0.409` MIB may not be in the MIB file.

Known Other issues

Bug ID	Description
281040	FortiManager may be unable to add FortiGate-1800D 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.

Policy and Objects

Known policy and objects issues

Bug ID	Description
271642	If `Used` contains two dynamic firewall addresses mapped to two separate devices, it may not work on an address group.
272429	In some cases, users may not be able to install changes to a firewall address object created with IP 255.255.255.255.
272958	If a Firewall Object is created with a + in the name, users may be able to edit it.
273658	When installing a policy package to a VDOM, the FortiManager may treats a LENC model with high encryption license as a regular LENC model. The install may revert the original VPN proposals and verification may not work.

Revision History

Known revision history issues

Bug ID	Description	Workaround
275350	When creating a new VDOM, a verification faliure on the `servercert` attribute may occur.	Run a `manual retrieve` if the failure occurs.

System Settings

Known system settings issues

Bug ID	Description
273390	Event Logs may show inconsistent entries for TACACS+ users and local users.

VPN Console

Known VPN Console issues

Bug ID	Description
271390	`Used` may produce an incomplete result for objects used in a VPN Console Topology.
271687	After upgrading the FortiManager, the pre-shared key that is specified with the random setting may change.

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:

FortiGuard Center update support

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	✓			
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
```

High Performance Network Security

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