FORTINET
High Performance Network Security

FortiManager - Release Notes

VERSION 5.2.9

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

December 29, 2016

FortiManager 5.2.9 Release Notes

02-529-388266 -20161229

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-09-21	Initial release.
2016-09-30	Updated to add the following resolved issue: 371045.
2016-12-06	Updated to add support for FortiOS 5.2.10.
2016-12-08	Updated description of 397220.
2016-12-29	Added special notice about Hyper-V FortiManager-VM running on an AMD CPU.

Introduction

This document provides the following information for FortiManager 5.2.9 build 780:

- Supported models on page 6
- Special Notices on page 7
- Upgrade Information on page 10
- Product Integration and Support on page 12
- Compatibility with FortiOS Versions on page 22
- Resolved Issues on page 23
- Known Issues on page 28
- FortiGuard Distribution Servers (FDS) on page 29

For more information on upgrading your device, see the FortiManager 5.2.9 Upgrade Guide.

Supported models

FortiManager version 5.2.9 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.2.9.

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.

FortiSandbox Support

Due to technical restriction, FortiManager currently only supports logging and FortiGuard updates for FortiSandbox.

Limitation on backing up and restoring FortiManager’s Database

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

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 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
```

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.

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
```

Upgrade Information

Upgrading to FortiManager 5.2.9

For information about upgrading your FortiManager device to 5.2.9, see *FortiManager 5.2.9 Upgrade Guide*.

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

Downgrading to previous firmware versions

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

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

FortiManager VM firmware

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

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Linux KVM

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

Microsoft Hyper-V Server

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

VMware ESX/ESXi

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

For more information see the FortiManager product data sheet available on the Fortinet web site, http://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 5.2.9 support

The following table lists 5.2.9 product integration and support information:

Web Browsers	- Microsoft Internet Explorer™ 11.0 - Mozilla Firefox version 48 - Google Chrome version 53 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	FortiManager 5.2.9 expects to support the following versions: - 5.2.6 to 5.2.10 FortiManager 5.2.9 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6 to 5.2.10, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.10 on page 22. - 5.2.0 to 5.2.5 FortiManager 5.2.9 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0 to 5.2.5, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 22. - 5.0.4 to 5.0.14 FortiManager 5.2.9 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.14, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 22. - 4.3.2 to 4.3.18 For the latest information, see FortiOS and FortiManager Compatibility at http://docs.fortinet.com/d/fortimanager-compatibility
FortiAnalyzer	- 5.2.0 and later - 5.0.0 and later
FortiCache	- 3.0.0 to 3.0.8
FortiClient	- 5.2.0 and later - 5.0.4 and later

FortiMail	• 5.2.8 • 5.1.5 to 5.1.6 • 5.0.8 to 5.0.10
FortiSandbox	• 2.1.3 • 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	• 5.3.8 • 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	✓	✓	✓	✓

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	GUI	Reports	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓	✓	
Chinese (Traditional)	✓	✓	
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 5.2.9.

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-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE,FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D,FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C,FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B **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-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC,FG-3810D-DC, FG-3950B-DC, FG-3951B-DC **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 **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-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FCT-5902D, 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-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FGT-3000D **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-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3815D-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 **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, FG-70D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5903C, FCT-5913	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-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-620B-LENC, FG-1000A-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC **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, FG-VMX **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

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

Model	Firmware Version
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

Supported FortiSandbox models

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

Supported FortiSwitch ATCA models

Model	Firmware Version
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0
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-3000E, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64	5.3
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 5.1 5.0

Supported FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D **FortiCache VM:** FCH-VM64	3.0 and later

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.2.9.

Compatibility issues with FortiOS 5.2.10

The following table lists interoperability issues that have been identified with FortiManager version 5.2.9 and FortiOS 5.2.10.

Bug ID	Description
397220	FortiOS 5.2.10 increased the maximum number of the firewall schedule objects for 1U and 2U+ appliances. As a result, a retrieve may fail if more than the maximum objects are configured.

Compatibility issues with FortiOS 5.2.5 or earlier

The following table lists interoperability issues that have been identified with FortiManager version 5.2.9 and FortiOS version 5.2.5.

Bug ID	Description
385924	FortiManager may try to install platform type as FPC220C or FPC225C within wireless profiles causing install to fail. Workaround: Users can delete all references on FPC220C or FPC225C within wireless profiles, and retrieve the updated configuration to FortiManager.

Resolved Issues

The following issues have been fixed in 5.2.9. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
356455	SNMPv3 passwords may be shorten to 32 characters.
306325	FortiManager always installs a secondary IP address when it has already been configured.
369127	FortiManager may report some valid IP addresses to be invalid.
365911	Installation may fail because of `ftgd-local-ratings`.
286467	Restoring an encrypted revision from FortiManager onto FortiGate may fail.
310915	FortiManager may incorrectly send IP settings to modem interface.
374585	FortiManager may not be able to create revisions when the `temp` folder is full.
371490	Users may not be able to edit an interface when its IP subnet overlaps with the IP of the `ha-mgmt-interface`.
377040	Session-helper table indices may not be maintained correctly on FortiManager.
374708	The disclaimer page limit for replacement message on FortiManager is different from that on FortiGate.
376426	Any changes in Webfilter's FortiGuard Settings may change the port range to `0-5`.
377913	The `tertiary-secret` setting in radius server configuration may not be installed to FortiGate.
365156	Interface may be created with a name containing a trailing space.
367000	The `use-management-vdom` setting in Radius options may be not set when per-device mapping is enabled.
374622	Changing the VDOM of an interface with existing dynamic mapping may create a second dynamic mapping for the same interface.

Bug ID	Description
366436	Users may not be able to change FortiGate's admin password from FortiManager.
365508	Users may not be able to add a static route for Transparent VDOM.
369743	Ha-priority for link health monitoring may cause installation to fail.
371315	GUI may display `loading aborted` error when users try to access the managed FortiSwitch page.
375319	Admin users with Read-Only profile may not be able to view revision diff when the workspace mode is set to normal.

Policy and Objects

Bug ID	Description
376262	Server-load-balance VIP with default port may be imported as port 0.
370248	FortiManager may display incorrect settings for FortiGuard categories if the Webfilter profile name contains `+`.
310196	Users may not be able to add or configure sections for explicit proxy policies.
357026	The *override* link may not be displayed if the blocked FortiGuard categories are pushed from FortiManager.
367113	Renaming an IP pool may cause installation failures.
369599	Following an upgrade from 5.2.2, FortiManager may not be able to install `ssl.vdom` interface that maps a zone to FortiGate.
367451	Changing a Zone name during import process may cause installation failures.
364210	Users may not be able to manually edit *Distinguished Name* in a user group when using a LDAP Remote Server.
367689	Users may not be able to modify the *Installation Target*.
157969	FortiManager may delete and then re-add the policies when firewall addresses are defined with associated-interface.
364216	The `match-vip` setting in a policy is not installed to FortiGate.
357099	Policies for policy-based IPSec VPN may not be installed to FortiGate when zone is used in destination interface.

Bug ID	Description
356939	Destination port and protocol values may be shown incorrectly when editing a web proxy service.
276987	In an Email Filter Profile, the *Log Email Summary* option may always be unchecked, and the *MAPI* option is missing.
289205	Users may not be able to view or set default status for custom IPS signature.
355374	If a user adds an IPS profile by right-clicking on a policy, an error message may be displayed.

Revision History

Bug ID	Description
301077	FortiManager may install outdated CRL to FortiGate.
371296	FortiManager may not install DHCP Relay servers for Virtual Switches to FortiGate.
381890	The `set active-auth-method` commands may be installed in a wrong order, causing installation failure.

Script

Bug ID	Description
364436	Duplicate objects may be allowed to be used.

Services

Bug ID	Description
364406	FGDSVR may run out of memory.
369636	Object `05000000IRDB00101` may not be shown on GUI.
370403	Firmware Manager concurrent install limit of 20.
383067	FortiManager GUI may show incorrect web filtering database size.

System Settings

Bug ID	Description
367428	Admin users with *Administrative Domain Read-Write* privileges may not be able to manage Administrative Domains if their *System Settings* privileges are *Read-Only* or *None*.
368149	Admin users may not be able to run diagnose sniffer when they have *Read-Only* permissions to *System Settings*.
369068	During an installation, FortiManager may generate incorrect out-of-sync config status in Event logs.
383819	HA members and non-FortiGate devices should be counted.
388017	After upgrade, device count may exceed the system's license and prevent users from adding or managing devices.

Others

Bug ID	Description
365346	The command `diagnose dvm check-integrity` may not be able to fix the errors reported in *Checking duplicate device vdoms*.
370925	The command `diagnose cdb check adom-integrity` may not work correctly for slave FortiManager.
373497	After a FortiGate is upgraded, the certificate authentication in VPN settings may be removed and be replaced by `PSK=NULL`.
373928	*FortiExtender* tab may not be displayed.
372455	The command `diagnose dvm proc list` may falsely report `PROCESS IS NOT RESPONDING`.
370121	Event log may not include FDS download logs.
375575	FortiManager may lose configuration and VM license after upgrade if the `tmp` folder is full.
377727	Portal Users may not be displayed from GUI.
373376	The `execute fmpolicy copy-adom-object` command may not work.

Bug ID	Description
379078	The fgfmsd daemon may run at 100% CPU.
380619	The command `diagnose dvm device list` may unexpectedly stop.
294103	When workspace mode is enabled, the *add-portal user* button may not be displayed.
372175	Removed maintainer account.
379110	FortiManager may not receive logs from a FortiGate HA cluster.
384882	FortiManager version should not be disclosed in the WSDL XML file.

Common Vulnerabilities and Exposures

Bug ID	Description
309902	FortiManager 5.2.9 is no longer vulnerable to the following CVE-Reference: • 2016-3193 Visit https://fortiguard.com/psirt for more information.
383809	FortiManager 5.2.9 is no longer vulnerable to the following TMP-Reference: • 2016-0023 Visit https://fortiguard.com/psirt for more information.
371045	FortiManager 5.2.9 is no longer vulnerable to the following CVE-References: • 2016-2176 • 2016-2109 • 2016-2108 • 2016-2107 • 2016-2106 • 2016-2105 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.2.9. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
381177	Users may not be able to view some corrupted devices.

Revision History

Bug ID	Description
378758	There may be `dmworker` crash when a lot of devices are in backup mode.

Script

Bug ID	Description
386069	Task Monitor may not report an error when FortiManager fails to run a script.

VPN Console

382045	SSLVPN portal changes may not be installed to FortiGate.

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	✓			
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
```

FORTINET®

High Performance Network Security