FortiManager 5.0.8
Release Notes

FortiManager 5.0.8 Release Notes

April 29, 2015

02-508-255548-20150429

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-10-08	Initial release.
2014-10-14	Corrected Upgrading from FortiManager 5.0.5 or earlier information.
2014-10-16	Added 0255814 to Resolved Issues.
2014-10-23	Updated the upgrade information section.
2015-01-14	Updated FortiOS support information.
2015-04-29	Updated the VM Partition Information in the Upgrade Information chapter.

Introduction

This document provides the following information for FortiManager version 5.0.8 build 0342:

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

Supported models

FortiManager version 5.0.8 supports the following models.

Table 1: Supported models

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

What's new in FortiManager 5.0.8

The following is a list of new features and enhancements in FortiManager version 5.0.8:

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

- Improved Web-based Manager consistency
- Policy table usability improvements
- Run Tcl script to access local databases
- Support Dynamic Mapping for ADOM objects - LDAP and TACACS+
- Added FG-92D and FWF-92D support
- Added FG-1000D support
- Added FG-5001D support
- Added FGR-60D support
- Added FGV-70D4 support

Special Notices

This section highlights some of the operational changes that administrators should be aware of in version 5.0.8.

Monitor upgrade process

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

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

ADOM upgrade

Upgrade is available for ADOM version 4.3 to migrate to version 5.0. Currently, there is no ADOM upgrade option for ADOM version 5.0 to move to version 5.2.

CLI commands for configuring dynamic objects

In version 5.0.7 and later, all dynamic objects are consolidated from devices to the ADOM database. For those users who wish to configure a dynamic mapping via a CLI script, the configuration for the mapping must be defined in the dynamic object under the `config dynamic_mapping` sub-tree. Also, the CLI script must be run on policy package instead of the device database. Below are some examples:

Example 1: Dynamic VIP

```
config firewall vip
  edit "vip1"
  …
  config dynamic_mapping
    edit "FW60CA3911000089"-"root"
      set extintf "any"
      set extip 172.18.26.100
      set mappedip 192.168.3.100
```

```
        set arp-reply disable
      next
    end
end
```

Example 2: Dynamic Address

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

Example 3: Dynamic Interface

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

FortiManager VM

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

Unregistered device table

In version 5.0.4 or earlier releases, the `config system global set unregister-pop-up` command is enabled by default. When a device is configured to send logs to FortiManager, the unregistered device table will be displayed. You can decide to promote the device now or at a later date.

In version 5.0.5 or later, the `config system global set unregister-pop-up` command is disabled by default. When a device is configured to send logs to FortiManager, the unregistered device table will not be displayed. Instead, a new entry *Unregistered Devices* will appear in the Device Manager tab under *All FortiGate*. You can then promote devices to specific ADOMs or use the right-click menu to delete the device.

FortiAnalyzer feature set

In version 5.0.5 or later, the FortiAnalyzer feature set (FortiView, Event Management, and Reports) is disabled by default. To enable the FortiAnalyzer feature set, enter the following CLI commands:

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

Enter `y` to continue, your FortiManager will reboot with the FortiAnalyzer features enabled.

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

In version 5.0.7 and later you can enable the FortiAnalyzer feature set in the Web-based Manager. Go to *System Settings* > *Dashboard*. In the *System Information* widget, beside *FortiAnalyzer Features*, select *Enabled*.

FortiGate firmware upgrade

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

System time on FortiManager VM (VMware)

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

Memory requirement for FortiManager VM64 (Hyper-V)

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

ADOM for FortiCarrier

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

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

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

FortiOS 5.0 override server setting for FortiGuard Services

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

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

Table 2 lists the ports used by FortiGuard Services.

Table 2: FortiGuard services ports

Port	Service
8890	Antivirus or IPS updates for FortiGate
53 or 8888	Web Filtering or Antispam queries for FortiGate
8891	Antivirus or IPS updates for FortiClient
80	Web Filtering or Antispam queries for FortiClient

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

Example 1: Antivirus/IPS

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

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

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

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

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

Example 2: Web filtering/Antispam

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

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

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

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

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

Update services provided to FortiMail 4.2 devices

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

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

Endpoint management

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

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

FortiManager VM license check

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

Multi-language display support

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

New hard disk drive partition layout

FortiManager version 5.0.0 introduced a new hard disk drive partition layout which is required for optimal usage and performance. Following an upgrade to FortiManager version 5.0.0 or later, a backup must be made and then the disk must be reformatted with following command:

```
execute format {disk | disk-ext4}
```

A format will erase all local logs, and FortiGuard database information. Backup any local event logs that you wish to keep. The FortiManager will then need to re-download all of the AV/IPS/AS/WF objects from the FortiGuard Distribution Servers (FDS) which may take up to half a day. During that time managed devices will not be able to obtain these services from the FortiManager. You should configure devices to point to a backup FortiManager or the FDS for these services.

Importing a FortiManager generated policy

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

- Global Header Policy
- Global Footer Policy
- VPN Console

Importing profile group and RADIUS dynamic start server

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

Push update in bi-directional static NAT

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

Configure the following settings on FortiManager:

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

Upgrade Information

Upgrading from FortiManager 5.0.6 or later

FortiManager version 5.0.8 supports upgrade from version 5.0.6 or 5.0.7.

FortiManager version 5.0.7 or later has re-sized the flash partition storing system firmware. If your FortiManager is running v5.0.6, you will need to change the hard disk provisioned size to more than 512 MB in your VM environment before powering on the FortiManager VM. The secondary firmware and System Settings stored in the partition is lost after upgrade. Please reconfigure System Settings as needed.

Upgrading your FMG-400B to version 5.0.8 requires you to use an interim step. You MUST upgrade to version 5.0.7 before upgrading to 5.0.8. For more information see the *FortiManager 5.0.7 Release Notes*. The upgrade path looks like this:

5.0.5 or earlier > 5.0.6 > 5.0.7 > 5.0.8

Upgrading from FortiManager 5.0.5 or earlier

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

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

Downgrading to previous firmware versions

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

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

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server 2008 R2/2012 virtualization environments.

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

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html.

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 v5.00 file folder.

Product Integration and Support

FortiManager 5.0.8 support

The following table lists version 5.0.8 product integration and support information.

Table 3: FortiManager 5.0.8 support

Web Browser	• Microsoft Internet Explorer versions 10 and 11 • Mozilla Firefox versions 31 and 32 • Google Chrome version 37 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 5.2.1 FortiManager 5.0.8 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. • 5.2.0 FortiManager 5.0.8 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues. • 5.0.4 to 5.0.10 FortiManager 5.0.8 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.10, with some minor interoperability issues. • 4.3.2 and later • 4.2.0 and later
FortiAnalyzer	• 5.2.0 • 5.0.0 and later
FortiMail	• 5.2.0 • 5.1.3 • 5.0.6
FortiWeb	• 5.3.0 • 5.2.3 • 5.1.4 • 5.0.6
FortiCache	• 3.0.0 and 3.0.1
FortiSwitch ATCA	• 5.0.0 and later • 4.3.0 and later • 4.2.0 and later

Table 3: FortiManager 5.0.8 support (continued)

FortiClient	• 5.2.0 and later • 5.0.4 and later
FortiSandbox	• 1.4.0 and later • 1.3.0 • 1.2.0 and later
Virtualization Software	
Microsoft	• Hyper-V Server 2008 R2 and 2012
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, and 5.5

Feature support

The following table lists FortiManager feature support for managed platforms.

Table 4: Feature support per platform

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

Language support

The following table lists FortiManager language support information.

Table 5: Language support

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

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

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

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

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager appliance running 5.0.8.

Table 6: Supported FortiGate models

Model	Firmware Version
FortiGate FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-94D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, 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-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-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FortiGate VM FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN FortiSwitch FS-5203B	5.2

Table 6: Supported FortiGate models (continued)

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-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5101C, FG-5001D 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-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-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-60D-POE, FWF-60D, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D FortiGate Rugged FGR-60D, FGR-100C FortiGateVoice FGV-70D4 FortiGate VM FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN FortiSwitch FS-5203B	5.0

Table 6: Supported FortiGate models (continued)

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-1000, FG-1000A, FG-1000AFA2, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001C, FG-5001FA2, FG-5002A, FG-5002FB2, FG-5005FA2, FG-5101C FortiGate DC FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-600C-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC FortiGate Low Encryption FG-20C-LENC, FG-40C-LENC, FG-50B-LENC, FG-51B-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-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

Table 6: Supported FortiGate models (continued)

Model	Firmware Version
FortiGate FG-30B, FG-50B, FG-51B, FG-60B, FG-80C, FG-80CM, FG-80CM, FG-82C, FG-100A, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-311B, FG-400A, FG-500A, FG-620B, FG-621B, FG-800, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001FA2, FG-5002A, FG-5002FB2, FG-5005FA2 FortiGate DC FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-621B-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC FortiGate Low Encryption FG-50B-LENC, FG-51B-LENC, FG-80C-LENC, FG-300C-LENC, FG-310B-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC FortiWiFi FWF-30B, FWF-50B, FWF-60B, FWF-60CX-ADSL-A, FWF-60CM, FWF-80CM, FWF-81CM, FWF-80CM, FWF-81CM FortiGate One FG-ONE FortiGate VM FG-VM	4.2

Table 7: Supported FortiCarrier models

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-3910B-DC, FCR-3950B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	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-3910B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	5.0

Table 7: Supported FortiCarrier models (continued)

Model	Firmware Version
FortiCarrier FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2 FortiCarrier DC FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	4.3
FortiCarrier FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2 FortiCarrier DC FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	4.2

Table 8: Supported FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-3000D, FAZ-3000E, FAZ-3500E, 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-HV	5.0

Table 9: Supported FortiMail models

Model	Firmware Version
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	5.2 5.1
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

Table 10: Supported FortiSandbox models

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

Table 11: Supported FortiSwitch ATCA models

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

Table 12: 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 5.2 5.1 5.0

Table 13: Supported FortiCache models

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

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in version 5.0.8.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.0.8 and FortiOS version 5.2.1.

Table 14: Compatibility issues with FortiOS 5.2.1

Bug ID	Description
0254828	Install logs show warning messages for `profile-protocol-options` when `oversize-limit` settings are larger than `uncompressed-oversize-limit` settings.

Compatibility issues with FortiOS 5.2.0

The following table lists interoperability issues that have been identified with FortiManager version 5.0.8 and FortiOS version 5.2.0.

Table 15: Compatibility issues with FortiOS 5.2.0

Bug ID	Description
0232983	User, User Group, and Device should be listed in the source or destination column.
0234563	The new VPN configuration wizard in FortiOS is not supported in FortiManager.
0246153	Remove AIM, ICQ, MSN, and Yahoo selections from the DLP sensor.

Compatibility issues with FortiOS 5.0.10

The following table lists interoperability issues that have been identified with FortiManager version 5.0.8 and FortiOS version 5.0.10.

Table 16: Compatibility issues with FortiOS v5.0.10

Bug ID	Description
0263526	Install fails for service `protocol-number`.

Compatibility issues with FortiOS 5.0.8 and 5.0.9

The following table lists interoperability issues that have been identified with FortiManager version 5.0.8 and FortiOS versions 5.0.8 and 5.0.9.

Table 17: Compatibility issues with FortiOS 5.0.8 and 5.0.9

Bug ID	Description
0249560	The `usb-wan` related settings cannot be retrieved by FortiManager.
0252696	FortiManager should not add a mesh interface and a virtual AP when creating a VDOM.

Compatibility issues with FortiOS 5.0.5

The following table lists interoperability issues that have been identified with FortiManager version 5.0.8 and FortiOS version 5.0.5.

Table 18: Compatibility issues with FortiOS 5.0.5

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

Compatibility issues with FortiOS 5.0.4

The following table lists interoperability issues that have been identified with FortiManager version 5.0.8 and FortiOS version 5.0.4.

Table 19: 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 version 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 version 5.0.5.
0226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS version 5.0.5.
0226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS version 5.0.5.

Table 19: Compatibility issues with FortiOS 5.0.4 (continued)

Bug ID	Description
0226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS version 5.0.5.
0230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS version 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS version 5.0.6.

Resolved Issues

The following issues have been fixed in version 5.0.8. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Table 20: Resolved device manager issues

Bug ID	Description
0204249	Import wizard should not allow user to map a single interface zone to a global zone that allows multiple interfaces.
0229635	FortiManager prompts an error when modifying a soft switch with only one interface.
0229738	FortiManager should be able to create two dead gateway detection profiles on the same interface.
0231105	FortiManager may not be able to create a new VDOM.
0244173	Users cannot discard custom replacement message changes leaving it blank.
0247034	FortiManager can no longer fully manage FortiGate device, showing the following error message after upgrading to version 5.0.7, `You cannot access this device/VDOM`.
0247463	FortiManager prompts a `Web Server Error500` when editing a FortiGate's interface with the FortiManager in offline mode.
0248850	FortiManager cannot add an IP address for a DHCP relay on an interface.
0249790	When clicking *View* from the device dashboard, some local user configurations are missing.
0250073	System may consume high CPU resources when moving devices across different ADOMs.
0250301	Users are unable to edit VDOM Resource Usage with an error message.
0251709	The browser tab may close after an install or importing a policy package.
0252886	Custom AP Profiles is missing the FAP-221C platform.
0254905	FortiManager returns a data error during an import policy package when there are more than 700 interfaces in the VDOM.

FortiOS Carrier ADOM

Table 21: Resolved FortiOS Carrier ADOM issues

Bug ID	Description
0247598	FortiManager may not be able to add a FortiOS Carrier device.
0251685	FortiManager should have a GTP column showing the profile used within a policy.
0252603	FortiManager does not accept GTP profile and APN names containing a dot character.
0247730	Using the right click menu from the source interface column to add a newly created address triggers an error message.

Global ADOM

Table 22: Resolved Global ADOM issues

Bug ID	Description
0251413	The default global firewall address, `gall`, is implicitly used by multicast policies.

Other

Table 23: Other resolved issues

Bug ID	Description
0241669	FortiManager is not able to print dynamic mapping by `print-global-object`.
0246074	HA may not be synchronized, and there is a show keep alive failure.
0247059	Resolved several SSH/SSL vulnerability issues.
0247383	The `diagnose dvm device dynobj` command cannot print device dynamic mappings when a VDOM belongs to a different ADOM.
0247580	The `diagnose cdb check objcfg-integrity` command may incorrectly identify errors after upgrading to version 5.0.7.
0247599	The `diagnose test deploymanager reloadconf` command does not indicate the cause of a failure and the session terminates abruptly.
0251003	Users cannot trigger a policy package installation preview via JSON APIs.
0251307	Using the JSON API to create a VDOM on an existing device, the `comments` field cannot be specified.
0251349	When upgrading an ADOM, SCTP anomalies are missing from DOS policies.

Policy and Objects

Table 24: Resolved policy and objects issues

Bug ID	Description
0223912	Section View is not available when a policy package is in a folder.
0224133	Install fails after changing a normal identity policy to a web-proxy policy.
0231969	Device Selection menu is inconsistent between device level and policy package level Installs
0235793	Users cannot delete the last listed zone in a VIP's *Source Interface Filter* list.
0238597	Dragging and dropping more than one scheduler into a policy should not be allowed.
0245267	The *Where used* feature does not work for predefined firewall service in a version 4.3 ADOM.
0246921	FortiManager prompts the error message, *TypeError*, when creating local categories for web filtering.
0247126	FortiManager should allow users to remove multiple installation targets at once.
0247352	FortiManager should support new IPS statements from IPSE 2.991.
0247458	It is impossible to choose a value for the *Comments* and *Change_Request_number* column filters.
0247475	FortiManager is unable to apply a column filter for the *Install On* field.
0247988	Dynamic mapping does not work for an address when the first octet is above 127.
0248019	It is impossible to unset the `session-ttl` value of a policy, and this change is pushed to the FortiGate device.
0248367	It is impossible to disable the traffic shaper option.
0248409	The *Web Filter Exempted Category* feature disappears from settings.
0248418	FortiManager does not allow spaces in the --pattern statement in an IPS custom signature.
0248531	The *Where_Used* tool does not show the correct information for *Local Categories*.
0248776	When modifying a multicast policy, the fields should populate according to what is currently set.
0248805	It should be possible to add a destination address to a web-proxy policy with subtype *User Identity* with right-click or drag and drop.
0250441	The right-click menu should not allow users to enable NAT on an explicit proxy causing installation failure.
0250576	The *Install On* column information is missing after upgrading to version 5.0.7.

Table 24: Resolved policy and objects issues (continued)

Bug ID	Description
0251001	Some dynamic address mappings are lost after upgrading to version 5.0.7.
0251156	The per-user black white list feature is not visible on FortiManager.
0252030	Renaming a firewall address object no longer displays it in the associated policy.
0255300	FortiManager should not add mailbomb and unhandled options to the antivirus profile.
0255814	When using a new version 5.0 ADOM default service *ALL*, an install to a version 5.0.6 FortiGate fails.

Revision History

Table 25: Resolved revision history issues

Bug ID	Description
0243939	Revision Diff highlights incorrect configuration changes.
0250442	Verification failed after configuring `vdom-property`.
0228112	Install fails due to an incorrect port setting for the NNTP `profile-protocol-options`.
0248279	After changing the dynamic zone's block intra-zone traffic setting, the change is not installed to FortiGate.
0250353	FortiManager may delete VPN policies if some VPN tunnels are configured in tunnel mode.

Script

Table 26: Resolved script issues

Bug ID	Description
0242431	Display a error message when a script fails due to duplicated members in firewall address group.
0243860	The CLI script window cannot be resized in Microsoft Internet Explorer.
0246699	The `getScriptLog` API always returns last executed script.
0251352	It should not be possible to create a LAG interface with members that are already in use.
0252400	FortiManager generates incorrect and inconsistent dynamic local certificate objects when creating it via a CLI script.

Services

Table 27: Resolved services issues

Bug ID	Description
0253070	FortiManager fails to push IRDB to FortiGate devices.

System Settings

Table 28: Resolved system settings issues

Bug ID	Description
0202585	Refreshing the dashboard causes additional `jsconsole` logins.
0235920	Users may not be able to use the CLI Java console and FortiManager prompts the error, `Too many concurrent connections`.
0247840	A user with read-only access should not be allowed to change their password.
0251713	SQL error messages should not be logged to the event log when deleting a policy package.
0252193	FortiManager should generate an event log entry when an ADOM is upgraded.

VPN Console

Table 29: Resolved VPN console issues

Bug ID	Description
0242085	FortiManager cannot bring up/down multiple tunnels at once.
0247444	The central IPsec table should show established IPsec tunnels for all managed devices or VDOMs.
0248170	FortiManager prompts an error when trying to add a new gateway in VPN console profiles.
0249200	FortiManager cannot change the IPsec phase1 remote gateway IP address.
0249440	A spoke with `add-route` deselected does not result in the setting being disabled.
0254260	IPsec VPN Phase 1 automatically adds a DES-MD5 proposal.
0255212	Spoke is changed to Hub if node settings are changed.

Known Issues

The following issues have been identified in version 5.0.8. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Table 30: Known device manager issues

Bug ID	Description
0252207	FortiManager does not support the FGR-90D.
0252914	FortiManager returns an HTML error when creating an interface for a device under Device Manager.

Other

Table 31: Other known issues

Bug ID	Description
0248167	Extending the LVM volume fails in FortiManager VM Hyper-V environments.

Policy and Objects

Table 32: Known policy and objects issues

Bug ID	Description
0251079	FortiManager may lose interface zone mappings.

Services

Table 33: Known services issues

Bug ID	Description
0249082	Service status does not reflect the GeoIP version.

Appendix A: FortiGuard

FortiGuard Distribution Servers (FDS) and services

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

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

FortiGuard Center update support

You can configure FortiManager version 5.0.8 as a local FortiGuard Distribution Server (FDS) to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Table 34: 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	✔		✔	
FortiMail	• 4.2.0 and later • 4.3.0 and later • 5.0.0 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	✔			

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
```