FORTINET®

High Performance Network Security

FortiManager Release Notes

VERSION 5.2.3

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 28, 2015

FortiManager 5.2.3 Release Notes

02-523-285539-20151028

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-07-30	Initial release.
2015-07-31	Added Compatibility issues with FortiOS 5.2.2 table to Compatibility.
2015-08-04	Added Bug 276245 to the Resolved Issues List.
2015-08-05	Added FortiSandbox 2.1.0 support to Product Integration and Support.
2015-08-10	Added Deleting a FortiGate with Dynamic Mappings information to Special Notices. Added Microsoft Hyper-V Server 2012 R2 Virtualization to Product Integration and Support. Added Bug IDs 288091 and 288226 to the Known Issues List.
2015-08-11	Added Per Device Mapping for Load Balance information to Special Notices.
2015-08-12	Added Bug 288655 to Known Issues List.
2015-08-18	Added additional information to Per-Device Mapping for Load Balance in Special Notices. Added Bug 288754 to Known Issues List.
2015-08-25	Added FG-3000D to Supported FortiGate 5.2 Models.
2015-08-26	Added Bug 289068 to Known Issues List.
2015-09-01	Added Compatibility Issues with FortiOS 5.2.3 table and information.
2015-09-02	Updated Web Browser information under Product Integration and Support.
2015-10-28	Added FG-600D to 5.2 Supported FortiGate Models. Added FG-900D to 5.0 Supported FortiGate Models.

Introduction

This document provides the following information for FortiManager 5.2.3 build 724:

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

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

Supported models

FortiManager version 5.2.3 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG64-AWS, and FMG-VM64-HV.

The following is a list of new features and enhancements in 5.2.3.

- Handling installation error improvements
- ADOM Management by Grouping

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

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.2.3.

Per-Device Mapping for Load Balance

Due to the Known Issue 288091 and 288754, FortiManager cannot manage Per-Device Mapping for Load Balance. If a Per-Device Mapping is configured on a Load Balance, FortiManager would prompt the *Loading Aborted* error message on the Virtual IP configuration page.

Deleting a FortiGate with Dynamic Mappings

Due to the Known Issue 288226, please conduct one of the following before deleting a FortiGate with Dynamic Mappings to avoid the *Loading Aborted* error:

1. Delete all Dynamic Mappings related to the FortiGate on all objects
2. Move the FortiGate device to another ADOM. FortiManager will remove all Dynamic Mappings,except for the Local Certificate. Please manually delete any related mappings for the Local Certificate and disable the *Per-Device Mapping* option. Then, you can re-enable the *Per-Device Mapping* option afterward.

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

FortiGate firmware upgrade

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

System time on FortiManager VM

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

Memory requirement for FortiManager VM64-HV

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

ADOM for FortiCarrier

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

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

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

FortiOS 5.0 override server setting for FortiGuard Services

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

This is applicable to FortiOS version 5.0 only. FortiOS version 4.3 and 5.2 have different behaviors.

Ports used by FortiGuard services

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

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

Example 1: Antivirus/IPS

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

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

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

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

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

Example 2: Web filtering/Antispam

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

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

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

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

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

Update services provided to FortiMail 4.2 devices

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

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

Endpoint management

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

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

FortiManager VM license check

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

Multi-language display support

FortiManager version 5.2.0 or later has restrictions on supporting a FortiGate device's multi-language display.

Importing a FortiManager generated policy

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

- Global Header Policy
- Global Footer Policy
- VPN Console

Importing profile group and RADIUS dynamic start server

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

Push update in bi-directional static NAT

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

Configure the following settings on FortiManager:

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

Upgrade Information

Upgrading from FortiManager 5.2.0, 5.2.1, and 5.2.2

FortiManager 5.2.3 supports upgrade from 5.2.0, 5.2.1 and 5.2.2.

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 5.2.3 support

The following table lists 5.2.3 product integration and support information:

Web Browsers	• Microsoft Internet Explorer™ 11.0 • Mozilla Firefox version 39 • Google Chrome version 43 Other web browsers may function correctly, but are not supported by Fortinet. Please make sure your computer's screen resolution is set to at least 1280x1024. Otherwise, web pages may not be displayed properly.
FortiOS/FortiOS Carrier	• 5.2.4 • 5.2.3 • 5.2.2 • 5.2.1 FortiManager 5.2.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 26. • 5.2.0 FortiManager 5.2.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility with FortiOS Versions on page 26. • 5.0.4 to 5.0.12 FortiManager 5.2.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.04 to 5.0.12, with some minor interoperability issues. For information, see Compatibility with FortiOS Versions on page 26. • 4.3.2 to 4.3.18
FortiAnalyzer	• 5.2.0 and later • 5.0.0 and later • 5.0.0 to 5.0.10
FortiCache	• 3.0.0 to 3.0.5
FortiClient	• 5.2.0 and later • 5.0.4 and later

FortiMail	• 5.2.4 • 5.1.5 • 5.0.8
FortiSandbox	• 2.1.0 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.3.7 • 5.2.4 • 5.1.4 • 5.0.6
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 6.2 • Linux KVM Redhat 6.5 • Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2 • OpenSource XenServer 4.2.5 **VMware** • ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0

To confirm that a device model or firmware version is supported by current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Feature support

The following table lists FortiManager feature support for managed platforms.

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

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		✔	
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 5.2.3.

Supported FortiGate models

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

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-300C-DC, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-900D, FG-1000C,FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B	5.0
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	
FortiGate Voice: FGV-40D2, FGV-70D4	
FortiSwitch: FS-5203B, FCT-5903C, FCT-5913C	

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

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-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
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

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	5.1.4
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

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	5.2.4 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 5.2.3.

Compatibility issues with FortiOS 5.2.3

The following table lists interoperability issues that have been identified with FortiManager version 5.2.3 and FortiOS version 5.2.3.

Bug ID	Description
289068	FortiManager may report a failure on the radio-2 setting with 802.11ac when installing a new VDOM. Workaround: Please run a `Retrieve` after the install.

Compatibility issues with FortiOS 5.2.2

The following table lists interoperability issues that have been identified with FortiManager version 5.2.3 and FortiOS version 5.2.2.

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

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.2.3 and FortiOS version 5.2.1.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263896	If it contains the certificate: `Fortinet_CA_SSLProxy` or `Fortinet_SSLProxy`, `retrieve` may not work as expected.

Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.3 and FortiOS version 5.2.0.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Compatibility issues with FortiOS 5.0.5

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.1 and FortiOS version 5.0.5.

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Compatibility issues with FortiOS 5.0.4

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.3 and FortiOS version 5.0.4.

Bug ID	Description
226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
226078	When the password length is increased to 128 characters, the installation fails.
226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.
226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS 5.0.5.

Bug ID	Description
226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Resolved Issues

The following issues have been fixed in 5.2.3. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
286227	After editing an interface filtered Zone, the Dynamic Zone Mapping pop-up may not only apply the change to filtered entries, and may delete the filtered entries upon validation.

GUI

Bug ID	Description
251593	When installing a configuration to the device within a ADOM backup, the install configuration pop-up window is repeatedly displayed.
256571	*Collapse All* action no longer works when using a Policy Package with large number of policies and/or Section Titles.
257534	FortiManager cannot import a firewall policy when the source interface is web-proxy and destination address is a VIP.
257959	Central IPSec does not display details for devices or VDOMs belonging to current a ADOM.
263459	Creating or importing local certificates causes issues with the SSL inspection profile.
270538	LDAP members with a configured workflow approval matrix wildcard is not able to approve, reject, or discard changes.
271286	FortiManager does not allow users to upload images larger than 6KB in a Replacement Message.
273658	If a high encryption license is installed on a FortiGate LENC model, the FortiManager does not treat it as a regular FortiGate and does not have all the encryptions available.
273905	When editing a managed FortiGate's interface in the v5.2 ADOM, the *fail:[object Object]* error message appears..

Bug ID	Description
274490	When a user cancels editing an interface, the FortiManager may direct to a different interface list.
274879	When editing an interface, and changing a VDOM and enabling DHCP at the same time, the FortiManager generates incorrect configuration and fails to install.
275022	Secondary IP for interface is not displayed in the Interface configuration page.
275577	FortiManager should not allow users to add VDOMs when they are not supported on a FortiGate platform.
276174	There is a typo when editing Interface/VLAN: *Map to Poilcy Interface*.
276629	FortiManager cannot add local certificate using the CLI-Only Objects Tree.
277034	FortiManager cannot manage DHCP Relay settings for SSID or switch port.
277778	After deleting a SSID from the WiFi template, the device's database does not update accordingly.
278483	FortiManager cannot select *main* or *aggressive* mode when defining a new `phase1`.
278484	Cloning static route returns: *runtime error 33: duplicate*.
278485	FortiManager is unable to set `phase2 auto-negotiate` parameter.
278493	When editing a zone from the GUI, the FortiManager is unable to delete the device interface.
278565	The web filter profile setting *Rate Images by URL* does not work.
278634	It is not possible to add an extra source address in an existing policy route.
278913	VDOM created on a FortiGate is not visible after a retrieve.

Global ADOM

Bug ID	Description
276064	FortiManager may not be able to assign a policy package to multiple ADOMs.

Other

Bug ID	Description
237815	FortiManager should be able to support IPv6 SNMP query and trap.
265754	FortiManager should have a reset command that does not reset the FortiManager's IP and route.
277392	Improve the performance to upgrade FortiManager when there are many dynamic objects.
279370	After upgrading, FortiManager cannot display policies if the policy package does not have a name.
280993	FortiManager does not print out all the debug messages in the console.
281172	When the `exe fmpolicy check-upgrade-object` command is run, FortiManager may stop working.
282094	FortiManager does not support `HTTP Expect: 100-continue` mechanism for JSON request.
276245	FortiManager may not be able to read or write from JSON APIs.

Policy and Objects

Bug ID	Description
212707	The Search field cursor on a policy package and on a Firewall address object is not in the same place.
255211	Scrolling for policies with the scroll wheel does not display all the policy entries.
256261	FortiManager always installs `profile-protocol-options` on a policy with IPS sensor.
265261	Users are not able to disable the SSL/SSH Inspection from Explicit Proxy policy.
268696	Where `Used` for service objects fails in Internet Explorer 11.
271390	Where `Used` produces incomplete result for objects used in a VPN Console Topology.
272958	Objects with name set with + plus sign cannot be edited from a Policy Package.

Bug ID	Description
273340	FortiManager uses high CPU resource when copying and pasting a policy.
275555	Installing a policy package always fails at Validation if policy package has a policy where *Action* is IPSEC.
275568	After submitting FortiClient XML configuration changes, the changes are not saved.
276354	NAT setting in IPv6 policy is changed after the policy is edited.
277061	Web URL filter entries having more than 65 characters are truncated.
277062	ADOM user gets removed from user group when the password is reset.
277071	There is a performance issue in the Display and Search interfaces.
277711	After selecting *Edit Interface Map*, the FortiManager does not list the Zone.
278089	When Workspace is enabled, FortiManager does not import the device. *Failed to commit changes to DB* error message may appear.
278357	FortiManager is unable to identify a device interface, when *per-device mapping* is enabled, to a policy interface or device zone.
278637	The FortiManager cannot edit an interface from the displayed Search Results.
279181	FortiManager cannot import an IPS custom signature.
279439	After removing members from a VIP group, the change is not be saved.
279534	FortiManager is unable to view or use imported CA certificates.
279900	FortiManager should display *Install On* targets in the CLI command: `execute fmpolicy print-adom-package <ADOM_ID> <POLICY_PACKAGE_ID> <Category> all.`
280112	The `.` character is not allowed for a LDAP username.
280607	If a global policy is configured when an address that has *per-device mapping* enabled, the mapping is lost on policy import.
280839	When importing zones into the Policy & ADOM database using CLI script, these zones do not appear in the GUI.
280875	In the SSL VPN Portal, users cannot disable the *Include Login History* option.
281201	Policy Package Column Settings are not saved per ADOM and administrative user.

Bug ID	Description
281289	FortiManager should be able to set the *Default Authentication Method* to *None* in Explicit Proxy Policy.
281511	FortiManager cannot display groups in LDAP Browsing.
281563	When setting change bonding to either 40MHz or 80MHz, FortiManager is unable to save the change.
283754	IPS signatures are not updated in the IPS sensor profiles.
284319	FortiManager may report the following error: *Install failed(dev-related info was changed, install it first)*.
284977	Pre-defined Bookmarks are not available when User Bookmarks is disabled.
285408	Toolbar Install Wizard is not grayed out when the *Save* button is active.
286706	The PAC file size may be inconsistent between FortiGate and FortiManager.

Revision History

Bug ID	Description
268732	When trying to do an install, FortiManager may try to unset the source IP of a FortiAnalyzer device.
271370	Policy package install fails as the FortiGate auto-deletes the HTTP prefix for the web filter.
274882	Installation fails due to a conflict between `/x` and `255.x.x.x netmask` notation.
277294	FortiManager may wipe-out all multicast objects and policies without warning.
279075	After upgrading, FortiManager sets up `tcp-portrange = 0` for some FortiOS versions.
280187	FortiManager is unable to retrieve 4.3 ADOM configurations. *Failed to reload configuration. Max entry.object wireless-controller* error message appears.
280193	When FortiGate HA is enabled, FortiManager discounts mac addresses for VDOM-link interfaces.
280324	FortiManager needs to be updated to add `set disable` and `set enable` when configuring `ftgd-wf` categories on v4.3 devices.

Bug ID	Description
281050	FortiManager sets `802.11n,g-only` band option as `802.11n g-only` to the wtp profile.
285530	FortiManager deletes the WANOPT peer from the server configuration.
286415	FortiManager keeps deleting or inserting *none* objects when installing 5.0 ADOM policies to FortiGates running FortiOS 5.2.
286872	FortiManager may continue to modify the global firewall policy UUID after an ADOM is upgraded from 5.0 to 5.2.

Script

Bug ID	Description
271615	FortiManager shows no record in script output after running a script via XML.
275359	FortiManager reports *runtime error 33: duplicate* when trying to append additional wildcard admins to the device database via device script.
275565	FortiManager should be able to change `fmg-source-ip` via a device database script.
280238	FortiManager may return CLI script errors with a VLAN message.

Services

Bug ID	Description
261736	Users should be able to configure *User-Agent* when fetching FortiGuard Content via a proxy.
279475	FortiManager may not be able to upgrade a FortiGate device's firmware using an image downloaded from FortiGuard.
282566	FortiManager is missing the row with firmware 5.2 in the table for *AV and Email filter update service for FortiMail*.

System Settings

Bug ID	Description
247941	On the HA slave, *System Settings* dashboard is blank with wildcard users with read-only profile login.
251003	FortiManager cannot receive a Policy Package Installation Preview via FMG JSON API
269919	Users are not able to delete a remote server with the right click menu.
275047	FortiManager is missing the installation history icon in the Task Monitor.
279186	When there is an on-going retrieve or installation task, the backup file becomes corrupted.
279415	Authentication times out after a few seconds with two-factor authentication.
281348	Upgrading ADOM from v5.0 to v5.2, FortiManager may delete all policy packages and objects.
283552	The JSON filter does not work in `/pm/pkg/adom/<adom>`.

VPN Console

Bug ID	Description
269222	FortiManager is unable to remove VPN Console > External Gateway > Hub IP value once it is configured.
277942	`Xauth authusrgrp` on `phase1` should be allowed to be empty and should not result in an error during policy installation.
280188	FortiManager cannot install policies after changing the Central VPN Gateway's protected subnet address object.

Known Issues

The following issues have been identified in 5.2.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

GUI

Bug ID	Description
284806	The search group function may not work when adding a device.
286686	When the WiFi template specifies a security mode requiring RADIUS, FortiManager may incorrectly try to set `auth usergroup` instead of `auth radius` in the VAP definition.

Other

Bug ID	Description
284528	Users may not be able to attain the Global Policy Package's ADOM Policy Package Exclusion List.

Policy and Objects

Bug ID	Description
285504	Section View may not be available if the policy package name contains the / or \ character.
286119	Dynamic mapping for global address object may not be installed onto the FortiGate device.
286824	FortiManager may display the application filter options even when selecting the specify applications option.
288091	FortiManager shows the *Loading Aborted* error on the Virtual IP page when a Per-Device Mapping is configured on a Load Balance object.
288226	If a FortiGate device is delete with Dynamic Mappings configured on the objects, some object pages may display the *Loading Aborted* error message.

Bug ID	Description
288655	The Policy Configuration page does not list a Zone if it contains *Per-Device Mapping* from multiple FortiGates. Workaround: Please configure the Default Mapping setting on the affected Zones.
288754	When Per-Device Mapping is configured on a Load Balance, the FortiManager may not be able to install Real Server Settings to the FortiGate.

Revision History

Bug ID	Description
285788	Installation may stop working if the CA certificate from ADOM database already exists on FortiGate with a different name.
286392	FortiManager may reset the IPS block duration if quarantine is disabled.

Script

Bug ID	Description
286111	TCL Script may stop working if the FortiGate SSH Port is another number than 22.

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

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.