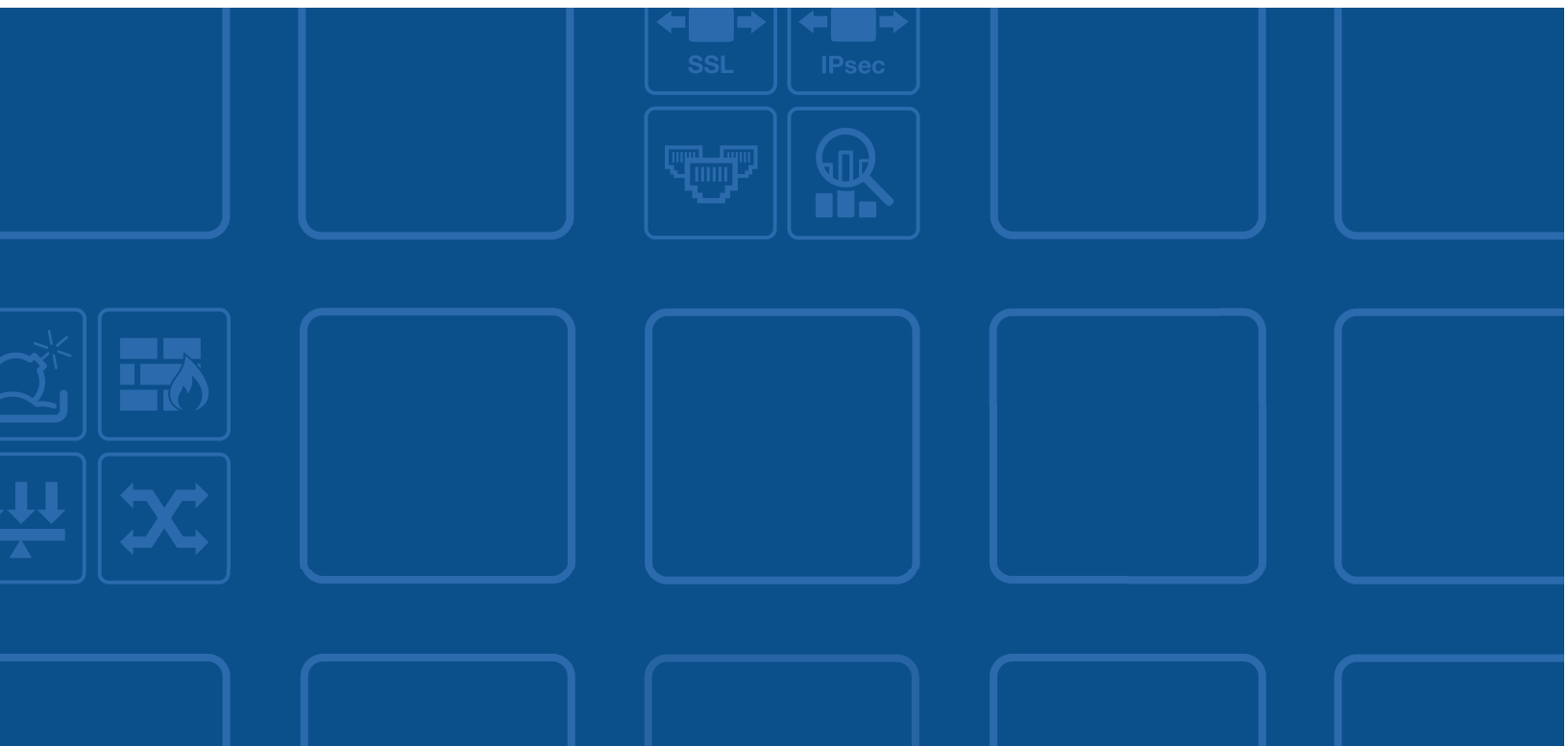
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.4.3



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

November 10, 2017

FortiOS 5.4.3 Release Notes

01-543-397185-20171110

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-12-21	Initial release of FortiOS 5.4.3.
2016-12-23	Added support for models FG-80E, FG-80E-POE, FG-81E, and FG-81E-POE.
2016-12-30	Updated supported build number for models FG-80E, FG-80E-POE, FG-81E, and FG-81E-POE.
2017-01-04	Updated *Introduction* > *What's new in FortiOS 5.4.3*.
2017-01-05	Removed bug 391786 from *Known Issues*.
2017-01-06	Removed bug 387216 from *Known Issues*.
2017-01-09	Added bugs 356330 and 398511 to *Known Issues*.
2017-01-17	Updated *Introduction* > *Special branch supported models*.
2017-01-26	Added bug 289491 to *Known Issues* > *Upgrade*.
2017-02-16	Updated *Special Notices* > *FortiGate units managed by FortiManager 5.0 or 5.2*.
2017-02-21	Removed bug 393267 from *Known Issues*.
2017-04-10	Added *Special Notices* > *Use of dedicated management interfaces (mgmt1 and mgmt2)*.
2017-05-15	Added build number for model FG-7000E.
2017-07-13	Added bug 440928 to *Known Issues* > *Upgrade*.
2017-11-10	Added bug 273973 to *Known Issues* > *Upgrade*.

Introduction

This document provides the following information for FortiOS 5.4.3 build 1111:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.4.3 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30D-POE, FG-50E, FG-51E, FG-60D, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-140D, FG-140D-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-5001C, FG-5001D
FortiWiFi	FWF-30D, FWF-30E, FWF-30D-POE, FWF-50E, FWF-51E, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE
FortiGate Rugged	FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM
FortiOS Carrier	FortiOS Carrier 5.4.3 images are delivered upon request and are not available on the customer support firmware download page.

Special branch supported models

The following models are released on a special branch of FortiOS 5.4.3. To verify that you are running the correct build, check the build number in *System Settings* > *Dashboard* > *System Information* > *Firmware Version* or in the CLI command `get system status` **Branch Point** field.

FGR-30D	is released on build 5861.
FGR-35D	is released on build 5861.
FGR-30D-A	is released on build 5861.
FG-30E-MI	is released on build 5858.
FG-30E-MN	is released on build 5858.
FWF-30E-MI	is released on build 5858.
FWF-30E-MN	is released on build 5858.
FWF-50E-2R	is released on build 5866.
FG-52E	is released on build 5862.
FG-60E	is released on build 5873.
FWF-60E	is released on build 5873.
FG-61E	is released on build 5873.
FWF-61E	is released on build 5873.
FG-80E	is released on build 5885.
FG-80E-POE	is released on build 5885.
FG-81E	is released on build 5885.
FG-81E-POE	is released on build 5885.
FG-90E	is released on build 5865.
FG-91E	is released on build 5865.
FWF-92D	is released on build 9482.
FG-100E	is released on build 5873.
FG-101E	is released on build 5873.

FG-200E	is released on build 5864.
FG-201E	is released on build 5864.
FG-2000E	is released on build 5860.
FG-2500E	is released on build 5860.
FG-3800D	is released on build 5859.
FG-7000E	is released on build 6182.

What's new in FortiOS 5.4.3

For a detailed list of new features and enhancements that have been made in FortiOS 5.4.3, see the *What's New for FortiOS* 5.4.3 document available in the Fortinet Document Library.

Special Notices

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

Default log setting change

For FG-5000 blades, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

FortiAnalyzer Support

In version 5.4, encrypting logs between FortiGate and FortiAnalyzer is handled via SSL encryption. The IPsec option is no longer available and users should reconfigure in GUI or CLI to select the SSL encryption option as needed.

Removed SSL/HTTPS/SMTPS/IMAPS/POP3S

SSL/HTTPS/SMTPS/IMAPS/POP3S options were removed from server-load-balance on low end models below FG-100D except FG-80C and FG-80CM.

FortiGate and FortiWiFi-92D Hardware Limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form
- IPv6 packets being dropped
- FortiSwitch devices failing to be discovered
- Spanning tree loops may result depending on the network topology

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed
- BPDUs are dropped and therefore no STP loop results
- PPPoE packets are dropped
- IPv6 packets are dropped
- FortiSwitch devices are not discovered
- HA may fail to form depending the network topology

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FG-3700DX

CAPWAP Tunnel over the GRE tunnel (CAPWAP + TP2 card) is not supported.

FortiGate units managed by FortiManager 5.0 or 5.2

Any FortiGate unit managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

FortiClient Support

Only FortiClient 5.4.1 and later is supported with FortiOS 5.4.1 and later. Upgrade managed FortiClients to 5.4.1 or later before upgrading FortiGate to 5.4.1 or later.

Note that the FortiClient license should be considered before upgrading. Full featured FortiClient 5.2, and 5.4 licenses will carry over into FortiOS 5.4.1 and later. Depending on the environment needs, FortiClient EMS license may need to be purchased for endpoint provisioning. Please consult Fortinet Sales or your reseller for guidance on the appropriate licensing for your organization.

The perpetual FortiClient 5.0 license (including the 5.2 limited feature upgrade) will not carry over into FortiOS 5.4.1 and later. A new license will need to be procured for either FortiClient EMS or FortiGate. To verify if a license purchase is compatible with 5.4.1 and later, the SKU should begin with FC-10-C010.

FortiClient (Mac OS X) SSL VPN Requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.3, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

FortiClient Profile Changes

With introduction of the Cooperative Security Fabric in FortiOS v5.4.1, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

In the FortiClient profile on FortiGate, when you set the *Non-Compliance Action* setting to *Auto-Update*, the FortiClient profile supports limited provisioning for FortiClient features related to compliance, such as AntiVirus, Web Filter, Vulnerability Scan, and Application Firewall. When you set the *Non-Compliance Action* setting to *Block* or *Warn*, you can also use FortiClient EMS to provision endpoints, if they require additional other features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

When you upgrade to FortiOS 5.4.1 and later, the FortiClient provisioning capability will no longer be available in FortiClient profiles on FortiGate. FortiGate will be used for endpoint compliance and Cooperative Security Fabric integration, and FortiClient Enterprise Management Server (EMS) should be used for creating custom FortiClient installers as well as deploying and provisioning FortiClient on endpoints. For more information on licensing of EMS, contact your sales representative.

FortiPresence

FortiPresence users must change the FortiGate web administration TLS version in order to allow the connections on all versions of TLS. Use the following CLI command.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

Log Disk Usage

Users are able to toggle disk usage between Logging and WAN Optimization for single disk FortiGates.

To view a list of supported FortiGate models, refer to the FortiOS 5.4.0 Feature Platform Matrix.

SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

FG-30E-3G4G and FWF-30E-3G4G MODEM Firmware Upgrade

The 3G4G MODEM firmware on the FG-30E-3G4G and FWF-30E-3G4G models may require updating. Upgrade instructions and the MODEM firmware have been uploaded to the Fortinet Customer Service & Support site. Log in and go to *Download* > *Firmware*. In the *Select Product* list, select *FortiGate*, and click the *Download* tab. The upgrade instructions are in the following directory:

.../FortiGate/v5.00/5.4/Sierra-Wireless-3G4G-MODEM-Upgrade/

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Upgrade Information

Upgrading to FortiOS 5.4.3

FortiOS version 5.4.3 officially supports upgrading from version 5.4.1 and later and 5.2.9 and later.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.4 Supported Upgrade Paths

Cooperative Security Fabric Upgrade

FortiOS 5.4.1 and later greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1 and later
- FortiClient EMS 1.0.1 and later
- FortiAP 5.4.1 and later
- FortiSwitch 3.4.2 and later

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Fabric - Upgrade Guide*
- *FortiOS 5.4.x Upgrade Guide for Managed FortiSwitch Devices*

  This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

FortiClient Profiles

After upgrading from FortiOS 5.4.0 to 5.4.1, your FortiClient profiles will be changed to remove a number of options that are no longer supported. After upgrading you should review your FortiClient profiles to make sure they are configured appropriately for your requirements and either modify them if required or create new ones.

The following FortiClient Profile features are no longer supported by FortiOS 5.4.1:

- Advanced FortiClient profiles (XML configuration)
- Advanced configuration, such as configuring CA certificates, unregister option, FortiManager updates, dashboard Banner, client-based logging when on-net, and Single Sign-on Mobility Agent

- VPN provisioning
- Advanced AntiVirus settings, such as Scheduled Scan, Scan with FortiSandbox, and Excluded Paths
- Client-side web filtering when on-net
- iOS and Android configuration by using the FortiOS GUI

It is recommended that FortiClient Enterprise Management Server (EMS) should used for detailed Endpoint deployment and provisioning.

Unified Disk Usage

FortiOS 5.4.3 changes the disk usage behavior upon upgrading from FortiOS 5.2. The table below describes the new logging and WAN Optimization disk usage for single and two disk FortiGate devices running FortiOS 5.4.3.

Single Disk Platforms (Logging or WAN Optimization)		
	Only Logging enabled	No change.
	Only WAN Optimization enabled	No change.
	Both Logging & WAN Optimization enabled	Disk is reserved for logging. If WAN Optimization is configured, the WAN Optimization cache is lost.
Two Disk Platforms (First disk reserved for Logging; second reserved for WAN Optimization)		
	Only Logging enabled on the first disk	No change.
	Only Logging enabled on the second disk	Logging is changed to the first disk. Logging data is lost on the second disk.
	Only WAN Optimization enabled on the first disk	WAN Optimization is changed to the second disk. WAN Optimization cache is lost on the first disk.
	Only WAN Optimization enabled on the second disk	Second disk reserved for WAN Optimization. First disk reserved for logging even when the log disk status CLI command is disabled: `log-disk-status=disable`.
	Both Logging & WAN Optimization enabled	First disk reserved for logging. Second disk reserved for WAN Optimization.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.3, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

When downgrading from 5.4 to 5.2, users will need to reformat the log disk.

Amazon AWS Enhanced Networking Compatibility Issue

Due to this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.4.1 or later image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

Downgrading to older versions from 5.4.1 or later running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

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

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

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

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*.

Product Integration and Support

FortiOS 5.4.3 support

The following table lists 5.4.3 product integration and support information:

Web Browsers	• Microsoft Edge 25 • Microsoft Internet Explorer 11 • Mozilla Firefox version 46 • Google Chrome version 50 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 25 • Microsoft Internet Explorer 11 • Mozilla Firefox version 45 • Apple Safari version 9.1 (For Mac OS X) • Google Chrome version 51 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	For the latest information, see the FortiManager and FortiOS Compatibility. You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	For the latest information, see the FortiAnalyzer and FortiOS Compatibility. You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.4.1 If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading the FortiGate.
FortiClient iOS	• 5.4.1
FortiClient Android and FortiClient VPN Android	• 5.4.0

FortiAP	• 5.4.1 and later • 5.2.5 and later Before upgrading FortiAP units, verify that you are running the recommended FortiAP version. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP*. If FortiAP is not running the recommended version, the *OS Version* column displays: *A recommended update is available*.
FortiAP-S	• 5.4.2 and later
FortiSwitch OS (FortiLink support)	• 3.5.0 and later
FortiController	• 5.2.0 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 2.1.0 and later • 1.4.0 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0254 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Standard
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	• 4.3 build 0164 (contact Support for download)
	  • Windows Server 2003 R2 (32-bit and 64-bit)
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard Edition
	  • Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExplorer	• 2.6 build 1083 and later. Some FortiGate models may be supported on specific FortiExplorer versions.

FortiExplorer iOS	• 1.0.6 build 0130 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 3.0.0 • 2.0.2 build 0011 and later
AV Engine	• 5.239
IPS Engine	• 3.299
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, and 2012 R2
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish (Spain)	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Microsoft Windows XP SP3 (32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2331
Microsoft Windows 10 (32-bit & 64-bit)	2331
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2331
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2331

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit/64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 46
Microsoft Windows 8/8.1 (32-bit/64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 46
Mac OS 10.9	Safari 7
Linux CentOS version 6.5	Mozilla Firefox version 46

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center 8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		

Product	Antivirus	Firewall
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved Issues

The following issues have been fixed in version 5.4.3. For inquires about a particular bug, please contact Customer Service & Support.

FG-3810D

Bug ID	Description
391998	CFP2 ports remains down after disconnecting and reconnecting fiber.

DLP

Bug ID	Description
367514	Executable files may not be blocked by DLP built-in .exe file-type filter.

FIPS-CC

Bug ID	Description
393649	SSH server rekey.

System

Bug ID	Description
392049	Cannot create the second IPv6 VIP, which has the same ext/int IP as the existing one, but different port-forwarding port.
393042	IPv6 traffic not distributed according to the lacp L4 algorithm.
392125	FortiGate to FortiManager backup config returned when with the `Management server is not configured` error message.
293751	After an HA failover, some multicast streams stop.
393034	The printout of `show sys interface` of FG-3700D begins with port5 instead of port1.
394582	Update geoip database to version 1.058(20161104).
389398	`Can't find xitem. Drop the response` in dhcp relay debug.
394471	Autoupdate tunneling password is shown in cleartext in CLI.

Bug ID	Description
393966	Trunk port doesn't work if the only port member is located on the second switch chip.
370349	Properly spin down SSD during graceful shutdown process.
388046	Process confsyncd memory leak.
395272	`unset password` is pushed during installation when FortiGate admin password was changed on FortiGate .
383748	Read-only admin of one or multiple VDOMs is able to see the entire configuration including other VDOMs.
388280	Some global configurations (admin, interface) are missing when global *prof_admin* backup full configuration.
395804	The first 20 CPUs became 100% busy when less than 18 million IPv6 sessions were established.
395796	FortiGate shows `Internet-service version(3) is not supported.` during signature update and device boot.
382996	Redundant type of interfaces are changing to aggregate after VDOM config restore.
396641	`Manualkey-interface` incorrect CLI help text.
310199	Delay destroying the fgfm session in error cases.
395796	Add a fix to support internet service version 1.
371672	When create a new `ftp-explicit-banner replacemsg`, it misses 220 FTP reply code.
369372	With low latency mode on NP6 unit enabled, only first 2 packets are correctly processed by FortiGate.
386626	TCP Session's timer consistently counting down until it goes expired while the traffic is passing through the unit.
393969	CPU spikes abnormally several times a day.
396574	FG-60E wan1/wan2 no longer come up after rebooting if the interface is down at boot.
387496	FSSO agent did not display all user group information.
389395	RDP-NLA connection to a windows server in multi domain environment overrides originator logon.

FortiSwitch

Bug ID	Description
393966	Trunk port does not work if the only VLAN member is on PoE interfaces.

FortiSwitch-Controller/FortiLink

Bug ID	Description
388024	Migrating the fix to limit FSWs based on FortiGate model on 5.4 branch.

FW

Bug ID	Description
389832	TCP/UDP ports 464 are missing in Service Group "Windows AD".

GUI

Bug ID	Description
375290	Fortinet Bar may not be displayed properly.
393267	Cannot edit existing Web Filter profile.
376049	Increase requireJS page load timeout.
363546	Error 500 when saving urlfilter list with 4900 entries.
388759	Can't view interface list via VDOM.
365667	PKI user groups are displayed incorrectly in the *Log & Report* > *Event Log* > *VPN* GUI.
390358	*Permission denied. Insufficient privileges* error is shown when opening *Security Profiles>Anti-Span*.
391111	Clicking the *Apply* button on *Explicit Proxy* page of one VDOM will disable *Explicit Proxy* of another VDOM.
369374	Config backup for non-global admins when VDOMs are disabled.
291231	Added monitor API method to deauthenticate individual firewall users.
399315	Fixed display of botnet entitlement in 5.4 UI.

HA

Bug ID	Description
391084	HA unable to sync inversed object entries.
388044	Four-member HA Cluster does not always re-converge properly when HB links are re-established
367158	FortiGate HA config failed to sync issue with fsso-polling.
388446	Session breaks when reboot master in PPPoE mode.
395407	When HA environment with pppoe failover, session down even if enabled session-pickup.
380279	`exec reboot` and `exec shutdown` triggered HA failover causes high packet loss.

SSL VPN

Bug ID	Description
307465	Fail to Copy & Paste through RDP when connected by SSL VPN web mode.
393698	SSL VPN web mode http/https SSO will keep trying even if the password is wrong.
393943	SSL VPN crash when connect to win2008 smb/CIFS bookmark with wrong password.
393758	Support for js to xml file containing html content.
387800	Skip fedtrul.js under owa.
396218	IE 11 fails to load OWA via SSL web portal.
391825	SSL VPN web mode does not work on port 80.
394936	Web-mode SSL VPN RDP bookmark does not allow connection without pre-populated username and password.
393980	libpthread is wrongly linked to RDP library.

IPsecVPN

Bug ID	Description
376135	DHCP process is crashing when more than 1500 users connect via dial up IPsec VPN with DHCP over IPsec feature enabled.
375910	`enc_npuid` and `dev_npuid` in `diag vpn tunnel list` output are reverse.
383939	Abnormal tracert through VPN tunnel on FG-30 and FG/FWF-60D.

WF

Bug ID	Description
394515	URL exempt/allow does not work as expected when certificate-inspection is used.
395365	Webfilter override present certificate resigned using SHA-1.
396005, 396078	wad crash and scan unit free one share memory randomly.

AV

Bug ID	Description
367514	Build-in AV engine 5.239.
371058	Properly detect executable (exe) file type and multiple file types.

WebProxy

Bug ID	Description
394844	When processing HTTP POST request with AV or IPS UTM is enabled, HTTP processing state is not correct.
382483	Unable to connect via SSH when Deep Scan is enabled in firewall policy for Putty.
301575	Proxyd crash on IMAP traffic.
395007	wad cannot process partial HTTP method correctly.
394314	inspect-all SSL profiles don't work after reboot in explicit proxy on AWS platform.

Log/Report

Bug ID	Description
373221	Can't clear log disk.
395471	Remove unsupported items from PCI-DSS checklist.
217208	Add log support for 802.1X authentication.
393970	crlevel wrong in raw traffic log for geolocation threat.
391786	`Logdiskless` FortiGate does not generate a log indicating a sandboxing result.

AppCtl

Bug ID	Description
394924	Disable kernel blocking of app-control identified sessions.

VM

Bug ID	Description
297361	FG-KVM-- between 2 10G-ports of FG-KVM04 test, It only got 2.75Gbps TCP throughput.
363439	KVM - UDP throughput of IMIX on KVM with VM08 is lower than it with VM01
372058	Upgrade to multiqueue virtio-net driver to improve network performance for FG-KVM.
394578	Print VM license not showing proper creation date.
394158	Merge AWS NFR feature for bootstrapping.
393434	iked hang and crash when receiving IKEv1 fragments with frag ID 0.

Router

Bug ID	Description
395789	Add jitter to BGP auto start timer to avoid oscillations in some cases.
375932	BFD `Path Down` message doesn't trigger BGP to clear the session.

Common Vulnerabilities and Exposures

Bug ID	Description
388594	FortiOS local admin password hashes could be obtained.

Known Issues

The following issues have been identified in version 5.4.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
374969	FortiSandbox FortiView may not correctly parse the FSA v2.21 tracer file(.json).
392200	Encrypted archive log is generated even though the function archive-log in antivirus profile is unset.

DLP

Bug ID	Description
379911	DLP filter order is not applied on encrypted files.

Endpoint Control

Bug ID	Description
375149	FortiGate does not auto update AV signature version while Endpoint Control is enabled.
374855	Third party compliance may not be reported if FortiClient has no AV feature.
391537	Buffer size is too small when sending a large vulnerability list to FortiGate.

Firewall

Bug ID	Description
364589	LB VIP slow access when cookie persistence is enabled.

FortiGate-3815D

Bug ID	Description
385860	FortiGate-3815D does not support 1GE SFP transceivers.

FortiRugged-60D

Bug ID	Description
375246	`invalid hbdev dmz` may be received if the default `hbdev` is used.
357360	DHCP snooping does not work on IPv6.
374346	Adding or reducing stacking connections may block traffic for 20 seconds.

FortiSwitch-Controller/FortiLink

Bug ID	Description
369099	FortiSwitch authorizes successfully, but fails to pass traffic until you reboot FortiSwitch.
357360	DHCP snooping may not work on IPv6.
304199	Using HA with FortiLink can encounter traffic loss during failover.

FortiView

Bug ID	Description
289376	Applying the filter *All* by using the right-click method may not work in the *All Sessions* page.
303940	*Web Site* > *Security Action* filter may not work.
373142	*Threat: Filter* result may not be correct when adding a filter on a threat and threat type on the first level.
366627	FortiView Cloud Application may display the incorrect drilldown *File and Session* list in the *Applications View*.
374947	FortiView may show empty country in the IPv6 traffic because country info is missing in log.
372350	*Threat view: Threat Type and Event* information are missing in the last level of the threat view.
375187	Using realtime auto update may increase chrome browser memory usage.
368644	*Physical Topology: Physical Connection* of stacked FortiSwitch may be incorrect.
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
372897	`Invalid -4` and `invalid 254` is shown as the submitted file status.

GUI

Bug ID	Description
289297	Threat map may not be fully displayed when screen resolution is not big enough.
303928	After upgrading from 5.2 to 5.4, the default flow based AV profile may not be visible or selectable in the Firewall policy page in the GUI.
374166	Using Edge cannot select the firewall address when configuring a static route.
365223	CSF: downstream FortiGate may be shown twice when it uses hardware switch to connect upstream.
373546	Only 50 security logs may be displayed in the *Log Details* pane when more than 50 are triggered.
375383	Policy list page may receive a `js` error when clicking the search box if the policy includes `wan-load-balance interface`.
375369	May not be able to change IPsec `manualkey config` in GUI.
374363	Selecting *Connect to CLI* from managed FAP context menu may not connect to FortiAP.
374521	Unable to *Revert* revisions on GUI.
374081	`wan-load-balance interface` may be shown in the address associated interface list.
355388	The *Select* window for remote server in remote user group may not work as expected.
373363	Multicast policy interface may list the `wan-load-balance interface`.
372943	Explicit proxy policy may show a blank for default authentication method.
375346	You may not be able to download the application control packet capture from the forward traffic log.
374224	The *Ominiselect* widget and *Tooltip* keep loading when clicking a newly created object in the *Firewall Policy* page.
374322	*Interfaces* page may display the wrong MAC Address for the hardware switch.
374247	GUI list may list another VDOM interface when editing a redundant interface.
374320	Editing a user from the *Policy* list page may redirect to an empty user edit page.
375036	The *Archived Data* in the *Sniffer Traffic* log may not display detailed content and download.
374397	Should only list `any` as destination interface when creating an explicit proxy in the TP VDOM.

Bug ID	Description
374221	SSL VPN setting portal mapping realm field misses the `/` option.
372908	The interface tooltip keeps loading the VLAN interface when its physical interface is in another VDOM.
374162	GUI may show the modem status as *Active* in the *Monitor* page after setting the modem to *disable*.
375227	You may be able to open the dropdown box and add new profiles even though errors occur when editing a *Firewall Policy* page.
375259	`Addrgrp` editing page receives a `js` error if `addrgrp` contains another group object.
374343	After `enable inspect-all in ssl-ssh-profile`, user may not be able to modify `allow-invalid-server-cert` from GUI.
372825	If the selected SSID has reached the maximum entry, the GUI will reset the previously selected SSID.
374191	The *Interface* may be hidden from the *Physical* list if its VLAN interface is a ZONE member in the GUI.
374525	When activating the *FortiCloud/Register-FortiGate*, clicking *OK* may not work the first time.
374350	Field *pre-shared key* may be unavailable when editing the IPsec dialup tunnel created through the VPN wizard.
374371	The IPS Predefined Signature information popup window may not be displayed because it is hidden behind the *Add Signature* window.
374183	The *Security* page does not have details for the *Forward Traffic* log for an IPS attack when displaying a FortiAnalyzer log.
374538	Unable to enable *Upload logs to FortiAnalyzer* after disabling it.
374373	*Policy View: Filter* bar may display the IPv4 policy name for the IPv6 policy.
365378	You may not be able to assign `ha-mgmt-interface` IP address in the same subnet as another port from the GUI.
374237	You may not be able to set a custom NTP server in the GUI if you did not config it in the CLI first.
393927	Policy List > *FQDN Object Tooltip* should show resolved IP addresses.
297832	Administrator with read-write permission for *Firewall Configuration* is not able to read or write firewall policies.

Bug ID	Description
283682	Cannot delete FSSO-polling AD group from LDAP list tree window in FSSO-user GUI.
365317	Unable to add new AD group in second FSSO local polling agent.
369155	There is no `Archived Data` tab for email attachment in the DLP log detail page.
356998	`urlfilter` list re-order on GUI does not work.
387640	`Duplicate entry found` when auto generate guest user.
379050	User Definition intermittently not showing assigned token.
395711	`pyfcgid` takes 100% of CPU when managed switch page displayed.
368069	Cannot select `wan-load-balance` or members for incoming interface of IPSec tunnel.

HA

Bug ID	Description
399115	ID for the new policy (when using edit 0) is different on master and on slave unit.
396938	Reboot of FortiGate HA cluster member with redundant HA management interface deletes HA configuration.
397171	FIB of VDOMs in vcluster2 is not synced to the slave.

IPSec

Bug ID	Description
393958	Shellshock attack succeeds when FortiGate is configured with `server-cert-mode replace` and an attacker uses `rsa_3des_sha`.
375020	IPsec tunnel Fortinet bar may not display properly.
374326	*Accept type: Any peer ID* may be unavailable when creating a IPsec dialup tunnel with a pre-shared key and `ikev1` in main mode.
386802	Unable to establish phase 2 when using address group/group object as quick mode selectors.
397386	Slave worker blades attempt to establish site to site IPsec VPN tunnel.
356330	Cross NP6-Chip IPSec traffic does not work in SLBC environment.

Logging & Report

Bug ID	Description
300637	MUDB logs may display *Unknown* in the *Attack Name* field under UTM logs.
374103	Botnet detection events are not listed in the *Learning Report*.
367247	FortiSwitch log may not show the details in the GUI, while in CLI the details are displayed.
374411	Local and Learning report web usage may only report data for outgoing traffic.
377733	*Results/Deny All* filter does not return all required/expected data.

Router

Bug ID	Description
393127	WLB measured-volume-based load balance does not work as expected after running for more than one day.
393623	Policy routing change not is not reflected.
385264	AS-override has not been applied in multihop AS path condition.
374306	Number of concurrent sessions affect the convergence time after HA failover.
299490	During and after failover, some MC Groups take up to 480 seconds to recover.
373892	ECMP(BGP) routing failover time.
397087	VRIP cannot be reached on 51E when it is acting as VRRP master.

SSL VPN

Bug ID	Description
304528	SSL VPN Web Mode PKI user might immediately log back in even after logging out.
303661	The Start Tunnel feature may have been removed.
375137	SSL VPN bookmarks may be accessible after accessing more than ten bookmarks in web mode.
374644	SSL VPN tunnel mode Fortinet bar may not be displayed.
395497	`https-redirect` for SSL VPN does not support realms.

Bug ID	Description
382223	SMB/CIFS bookmark in SSL VPN portal doesn't work with DFS Microsoft file server error "Invalid HTTP request".
366291	High CPU usage by SSL VPN.

System

Bug ID	Description
304199	FortiLink traffic is lost in HA mode.
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
290708	`nturbo` may not support CAPWAP traffic.
372717	Unable to access FortiGate GUI via `https` using low ciphers.
364280	User cannot use `ssh-dss` algorithm to log in to FortiGate via SSH.
371320	`show system interface` may not show the *Port* list in sequential order.
372717	`admin-https-banned-cipher` in `sys global` may not work as expected.
371986	NP6 may have issue handling fragment packets.
287612	Span function of software switch may not work on FortiGate-51E/FortiGate-30E.
355256	After reassigning a hardware switch to a TP-mode VDOM, bridge table does not learn MAC addresses until after a reboot.
393395	The role of new VAP interface should be set as LAN.
393343	Remove botnet filter option if interface role is set to LAN.
392960	FOS support for V4 BIOS.
377192	DHCP request after lease expires is sent with former unicast IP instead of 0.0.0.0 as source.
397642	FG5HD a-p cluster, LDAP authentication fails for users members of huge amount of LDAP groups.
381363	Empty username with Radius 802.1x WSSO auth.
354490	False positive sensor alarms in Event log.
398511	Sometimes the FG-5001D model selects a link-down port as an active slave of the redundant interface which causes system instability.

Upgrade

Bug ID	Description
269799	`Sniffer config` may be lost after upgrade.
273973	When upgrading from 5.2 to 5.4, the Central NAT feature cannot be upgraded. After the upgrade, reconfigure the Central NAT feature. Please see the configuration examples in the FortiOS Handbook available in the Fortinet Document Library.
289491	When upgrading from 5.2.x to 5.4.0, port-pair configuration may be lost if the `port-pair` name exceeds 12 characters.
440928	Image release label patch always shows as '0' for FGT with image from v5.4.1 to v5.4.4

Visibility

Bug ID	Description
374138	FortiGate device with VIP configured may be put under Router/NAT devices because of an address change.

VM

Bug ID	Description
364280	`ssh-dss` may not work on FG-VM-LENC.
378421	Committing any change on SSL VPN Settings over web page returns `error:500`.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET

High Performance Network Security