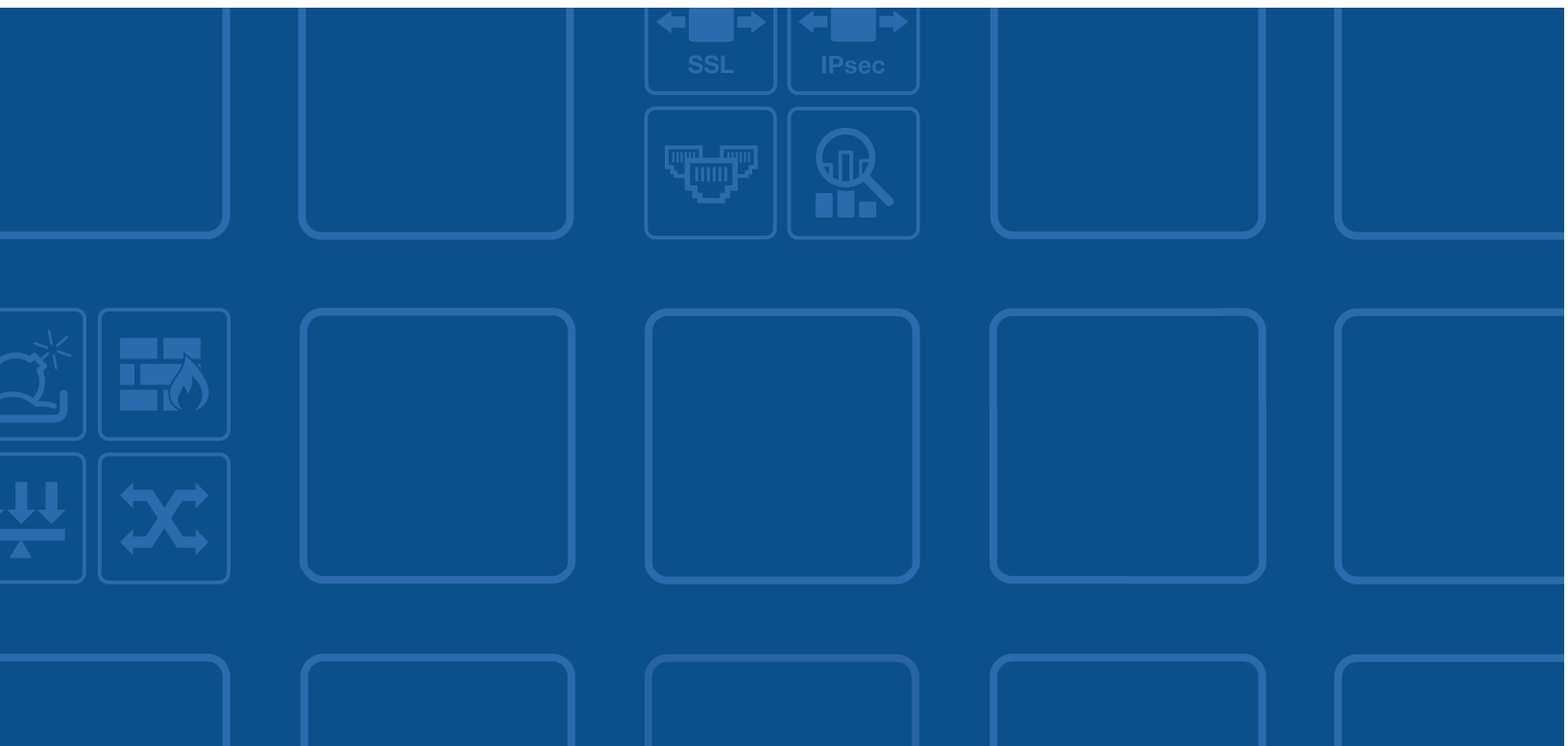
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.4.4



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 5.4.4 Release Notes

01-544-405841-20171110

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-02-10	Initial release of FortiOS 5.4.4.
2017-02-16	Added FortiOS NP4Lite supported models. Updated bug 382657 that it refers to MP4Lite models only. Updated bug 387014 that it refers to FG-1500D only.
2017-02-21	Removed bug 393267 from *Resolved Issues* since this bug has been resolved in a previous release.
2017-02-21	Added bug 408366 to *Known Issues* > *Upgrade*.
2017-03-02	Updated command in *Special Notices* to `config system global`.
2017-03-13	Updated bug 299490 to clarify that MC is multicast.
2017-04-03	Added 374501 to *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2017-04-10	Added *Special Notices* > *Use of dedicated management interfaces (mgmt1 and mgmt2)*.
2017-04-12	Updated *Product Integration and Support* > *SSL VPN support*.
2017-06-02	Moved affected models for FortiOS NP4Lite from *Introduction* > *Supported models* to *Resolved Issues* 382657.
2017-07-12	Added bug 424215 to *Known Issues* > *System*.
2017-07-13	Added bug 440928 to *Known Issues* > *Upgrade*.
2017-09-18	Added 413699 to *Known Issues* > *Upgrade*.
2017-11-10	Added bug 273973 to *Known Issues* > *Upgrade*.

Introduction

This document provides the following information for FortiOS 5.4.4 build 1117:

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

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.4.4 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 FortiOS 5.4.4 supports the additional CPU cores through a license update on the following VM models: • VMware 16, 32, unlimited • KVM 16 • Hyper-V 16, 32, unlimited
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM
FortiOS Carrier	FortiOS Carrier 5.4.4 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 5.4.4. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch Point` field shows 1117.

FGR-30D	is released on build 7603.
FGR-35D	is released on build 7603.
FGR-30D-A	is released on build 7603.
FGT-30E-MI	is released on build 5971.
FGT-30E-MN	is released on build 5971.
FWF-30E-MI	is released on build 5971.
FWF-30E-MN	is released on build 5971.
FWF-50E-2R	is released on build 7607.
FGT-52E	is released on build 6011.
FGT-60E	is released on build 6003.
FWF-60E	is released on build 6003.
FGT-61E	is released on build 6003.
FWF-61E	is released on build 6003.
FGT-80E	is released on build 6003.
FGT-81E	is released on build 6003.
FGT-81E-POE	is released on build 6003.
FGT-90E	is released on build 6019.
FGT-91E	is released on build 6019.
FWF-92D	is released on build 7602.
FGT-100E	is released on build 6003.
FGT-100EF	is released on build 6003.
FGT-101E	is released on build 6003.

FGT-200E	is released on build 5968.
FGT-201E	is released on build 5968.
FGT-2000E	is released on build 6020.
FGT-2500E	is released on build 6020.
FGT-3800D	is released on build 6013.
FGT-VM64	is released on build 7605.
FGT-VM64-KVM	is released on build 7605.
FGT-VM64-HV	is released on build 7605.

What's new in FortiOS 5.4.4

For a detailed list of new features and enhancements that have been made in FortiOS 5.4.4, see the *What's New for FortiOS* 5.4.4 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 system 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 5.4.4, 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, 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 5.4.4

FortiOS version 5.4.4 officially supports upgrading from version 5.4.2 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.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.4, 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 5.4.4 support

The following table lists 5.4.4 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 current recommended FortiAP version. To do this in the GUI, go to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP*. If your FortiAP is not running the recommended version, the *OS Version* column displays the message: *A recommended update is available*.
FortiAP-S	• 5.4.1 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	• 3.305
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, 2012 R2, and 2016
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, 6.0, and 6.5
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 7 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit) Microsoft Windows 10 (64-bit)	2333
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2333
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2333

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 Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 52 Google Chrome version 56
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 52 Google Chrome version 56
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 52
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 52 Google Chrome version 56
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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	✔	✔

Product	Antivirus	Firewall
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		
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 5.4.4. For inquires about a particular bug, please contact Customer Service & Support.

AV

Bug ID	Description
370074	HTTP evader tool - AV evasion through manipulating HTTP content-encoding.

DLP

Bug ID	Description
379911	DLP filter order is not applied to encrypted files.
367514	Executable files may not be blocked by DLP built-in `.exe` file-type filter.

FortiView

Bug ID	Description
289376	Applying the filter *All* by using the right-click method may not work in the *All Sessions* page.

GUI

Bug ID	Description
374221	SSL VPN setting portal mapping realm field misses the `/` option.
374162	GUI may show the modem status as `Active` in the `Monitor` page after setting the modem to disable.
378421	Committing any change on SSL VPN Settings over web page returns `error:500`.
356998	`urlfilter` list re-order on GUI does not work.
396783	Disable GUI support for Domain/IP reputation feature.

HA

Bug ID	Description
401745	Master can't sync with slave after updating OS from b1099.

Log & Report

Bug ID	Description
397132	Log rate is only 30k without any log lost on 3700D.
369778	The FWF_90D daemon report takes 99% of CPU time.
387014	EXT2 and EXT3 Errors from Console on 1500D.
400871	Changes to support Log Message Reference.

Switch-Controller

Bug ID	Description
395711	`pyfcgid` takes 100% of CPU when managed switch page displayed.
400700	FortiLink is unstable - 1 min. disconnect/reconnect.

SSL VPN

Bug ID	Description
366291	High CPU usage by SSL VPN.
397654	Intranet website opens in separate tabs in web-mode SSLVPN.

Firewall

Bug ID	Description
396527	Policy does not work as intended when there are two IPv6 VIPs which has the same `mappedip` and different `extip`.

IPS

Bug ID	Description
396658	IPS signature count decreases from ~10k to ~5k after FGT reboot.

IPsecVPN

Bug ID	Description
384334	`unregister_netdevice:` showing up on console after ha failover if flushing ipv6 advpn spoke.

Bug ID	Description
385658	DPD interoperability issue with Huawei eNodeB.
396041	Tunnel interface loses its config after reboot on 50E.

Users

Bug ID	Description
397642	FGT5HD a-p cluster, LDAP authentication fails for users members of huge amount of LDAP groups.
400065	The FSSO users were not able to pickup by firewall policy.

System

Bug ID	Description
401241	SSL handshake fails when WAD needs to update the session ticket.
401886	Update geoip database to version 1.060(20170106).
398511	Sometimes the FG-5001D model selects a link-down port as an active slave of the redundant interface which causes system instability.
391516	Add Franklin USB700 Modem support.
289738	FortiGate now supports Verizon 4G LTE USB Modem U620L.
386859	Netgear/Sierra AC340U wireless modem cards do not attach to USB serial properly on FG30E/50E.
384831	CDC Ethernet USB modem not working on Kernel 3.2 devices.
396472	Checksum control is not working when upgrading firmware.
370586	Add CLI commands to configure limited IPsec engine on NP6.

Router

Bug ID	Description
397628	Internet-service based routing not working.
402019	Policy Route member based is not updated untill config change or `lnkmtd` is restarted.

WebProxy

Bug ID	Description
398297	WAD does not forward http POST with data but reset the connection when action is allow.
398267	WAD crashes with singal 11 when App ctrl is used in webproxy policy.
400556	WAD dispatcher incorrectly count active file-descriptors.

Common Vulnerabilities and Exposures

Bug ID	Description
374501	FortiOS 5.4.4 is no longer vulnerable to the following CVE Reference: • 2016-0723 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.4.4. 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.

Endpoint Control

Bug ID	Description
375149	FGT 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.

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.

FortiGate-92D

Bug ID	Description
267347	FortiGate-92D does not support Hardware switch.

FortiGate and FortiWifi E Series

Bug ID	Description
413699	In some FortiGate and FortiWifi E series models, the default *Inspection Mode* is flow-based instead of proxy-based. Affected models: FG-60E, FG-61E, FWF-60E, FWF-61E, FG-80E, FG-81E, FG-80E-POE, FG-81E-POE, FG-100E, FG-101E, FG-100EF, FG-140E, FG-140E-POE.

FortiRugged-60D

Bug ID	Description
375246	`invalid hbdev dmz` may be received if the default `hbdev` is used.

FortiSwitch-Controller/FortiLink

Bug ID	Description
357360	DHCP snooping may not work on IPv6.
374346	Adding or reducing stacking connections may block traffic for 20 seconds.
369099	FortiSwitch authorizes successfully, but fails to pass traffic until you reboot FortiSwitch.
304199	Using HA with FortiLink can encounter traffic loss during failover.

FortiView

Bug ID	Description
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 is 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.

Bug ID	Description
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.
374166	Using Edge cannot select the firewall address when configuring a static route.
374081	`wan-load-balance interface` may be shown in the address associated interface list.
374521	Unable to *Revert* revisions on GUI.
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.
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.
365223	CSF: downstream FGT 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`.
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.

Bug ID	Description
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.
372908	The interface tooltip keeps loading the VLAN interface when its physical interface is in another VDOM.
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.
374525	When activating the *FortiCloud/Register-FortiGate*, clicking *OK* may not work the first time.
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.
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.

Bug ID	Description
297832	Administrator with read-write permission for *Firewall Configuration* is not able to read or write firewall policies.
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.
368069	Cannot select `wan-load-balance` or members for incoming interface of IPSec tunnel.
378802	Clicking *Archived File* button in *Archive Data* tab brings a webpage with "null".

HA

Bug ID	Description
369437	HA Sync status icon is missing for Slave's GUI.
397171	FIB of VDOMs in vcluster2 is not synced to the slave.
399115	ID for the new policy (when using edit 0) is different on master and on slave unit.
396938	Reboot of FGT HA cluster member with redundant HA management interface deletes HA configuration.

IPSec

Bug ID	Description
393958	Shellshock attack succeeds when FGT 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.

Bug ID	Description
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.
377255	Can't read UTM details on log panel when set location to FortiAnalyzer.
386742	Missing deny traffic log when user traffic is blocked by NAC quarantine.

Router

Bug ID	Description
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 multicast 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.

Bug ID	Description
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.
382223	SMB/CIFS bookmark in SSL VPN portal doesn't work with DFS Microsoft file server error "Invalid HTTP request".
394272	SSL VPN proxy mode can't proxy some web server url normally

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.
381363	Empty username with Radius 802.1x WSSO auth.

Bug ID	Description
354490	False positive sensor alarms in Event log.
383126	50E/51E TP mode - STP BPDU forwarding destined to 01:80:c2:00:00:00 has stopped after warm/cold reboot.
310665	SNMP Interfaces dropdown is obsolete on some platforms.
382657	ICMP Packets bigger than 1418 bytes are dropped when offloading for IPSec tunnel is enabled. Affected models: FG-30D, FG-60D, FG-70D, FG-90D, FG-90D-POE, FG-94D, FG-98D, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FWF-30D, FWF-60D, FWF-90D, FWF-90D-POE.
394067	Improve displaying the warning: *File System Check Recommended*.
424215	FG-80C halts during boot after upgrade from 5.2.10 to 5.4.4.

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.
408366	FGT_VM platforms cannot do uninterruptible upgrade in HA mode. Workaround: Upgrade each cluster member separately.
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 FGT-VM-LENC.

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