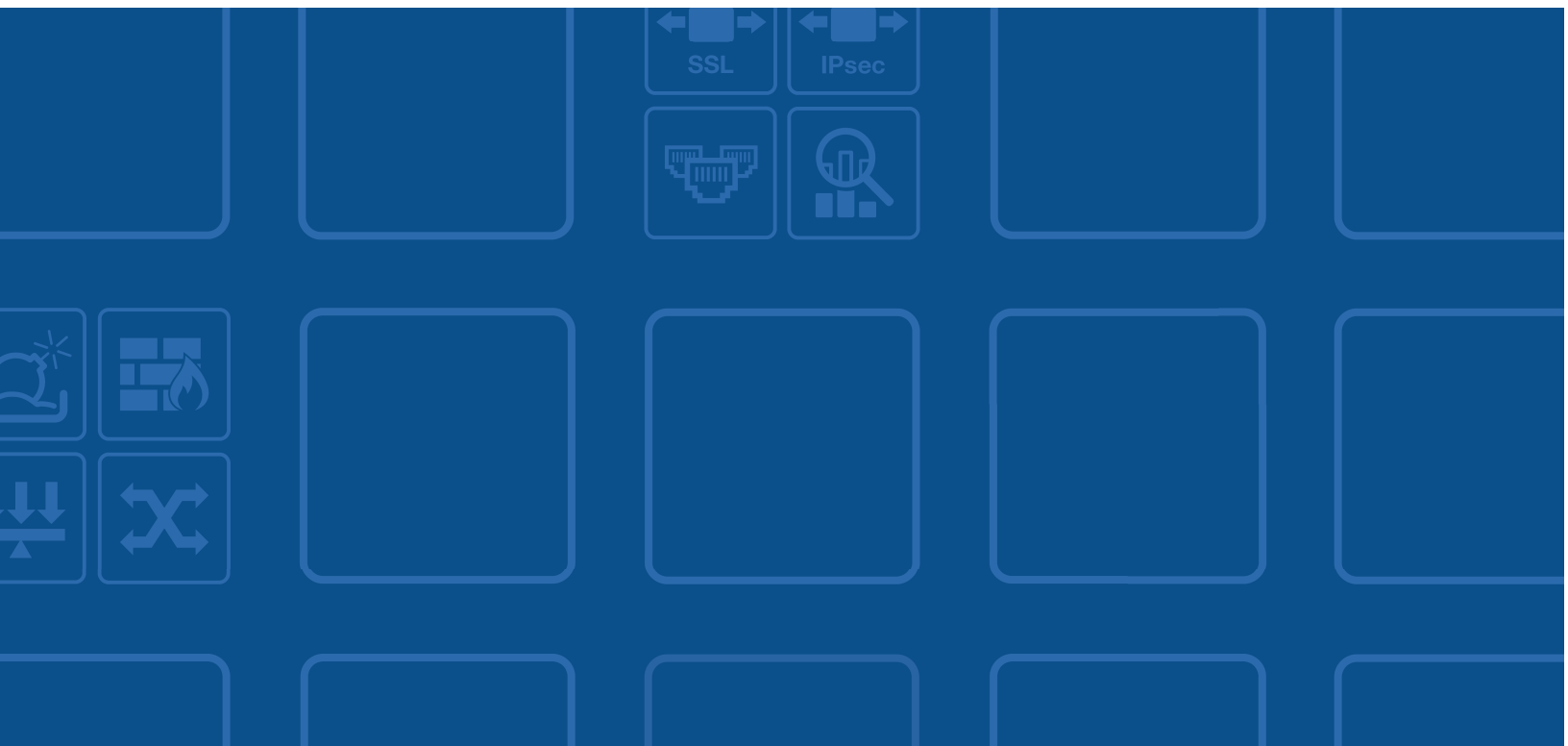
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.4.2



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 5.4.2 Release Notes

01-542-392095-20171110

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-11-01	Initial release of FortiOS 5.4.2.
2016-11-02	Updated to clarify upgrade path.
2016-11-04	Updated list of supported models, added 394515 to Known Issues, and added FG-30E-3G4G and FWF-30E-3G4G MODEM Firmware Upgrade to Special Notices.
2016-11-17	Removed 372770 and updated 373707 in Resolved Issues.
2016-11-22	Added 367040 to Resolved Issues. Removed note about FortiAP-421E and FortiAP-423E from the Product Integration and Support section.
2016-11-24	Updated information about special branch support for FWF-92D.
2016-11-25	Updated 385669 and added 392037 to Resolved Issues.
2016-11-30	Added 389206 to Resolved Issues.
2016-12-02	Fixed incorrect CVE number for 367040 in Resolved Issues.
2016-12-12	Added 370360 to Resolved Issues.
2016-12-16	Removed Model-60D Boot Issue from the Upgrade section.
2017-01-06	Removed 387216 from Known Issues.
2017-01-26	Added 289491 to Known Issues > Upgrade section.
2017-02-16	Updated Special Notices > FortiGate units managed by FortiManager 5.0 or 5.2.
2017-11-10	Added 273973 to Known Issues > Upgrade.

Introduction

This document provides the following information for FortiOS 5.4.2 build 1100:

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

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.4.2 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 5.4.2 images are delivered upon request and are not available on the customer support firmware download page.

The following models are released on a special branch based off of FortiOS 5.4.2. As such, the *System > Dashboard > Status* page and the output from the `get system status` CLI command displays the build number.

FGR-30D	is released on build 5759.
FGR-35D	is released on build 5759.
FGR-30D-A	is released on build 5759.
FGT-30E-MI	is released on build 5813.
FGT-30E-MN	is released on build 5813.
FWF-30E-MI	is released on build 5813.
FWF-30E-MN	is released on build 5813.
FWF-50E-2R	is released on build 5756.
FGT-52E	is released on build 5762.
FGT-60E	is released on build 5769.
FWF-60E	is released on build 5769.
FGT-61E	is released on build 5769.
FWF-61E	is released on build 5769.
FGT-90E	is released on build 5755.
FGT-91E	is released on build 5755.
FWF-92D	is released on build 7364.
FGT-100E	is released on build 5769.
FGT-101E	is released on build 5769.
FGT-200E	is released on build 5808.
FGT-201E	is released on build 5808.
FGT-2000E	is released on build 5760.
FGT-2500E	is released on build 5760.
FGT-3800D	is released on build 5765.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 1100.

What's new in FortiOS 5.4.2

For a detailed list of new features and enhancements that have been made in FortiOS 5.4.2, see the *What's New for FortiOS* 5.4.2 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 5.4.2, 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/

Upgrade Information

Upgrading to FortiOS 5.4.2

FortiOS version 5.4.2 officially supports upgrading from version 5.4.0 and later and 5.2.8 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 and later, 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 and later:

- 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 5.4.2 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 5.4.2.

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 5.4.2, 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 5.4.2 support

The following table lists 5.4.2 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 • 5.2.5 and later You should verify what the new FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller > Managed Access Points > Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.
FortiAP-S	• 5.4.2 and later
FortiSwitch OS (FortiLink support)	• 3.4.2 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 0250 and later (needed for FSSO agent support OU in group filters)
	  • 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	• 5.234
IPS Engine	• 3.294
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)	2329
Microsoft Windows 10 (32-bit & 64-bit)	2329
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2329
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2329

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		
F-Secure Internet Security 2011	✔	✔

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

FortiGate-60D

Bug ID	Description
372629	Hardware issue of FG-60D cause config lost

FortiGate-80D

Bug ID	Description
373153	FG-80D should support jumbo frame on new kernel
376656	FG-80D change port speed does not take effect

FortiGate-500D

Bug ID	Description
371098	VLAN counters match physical port if NP6 offloading is disabled

FortiGate-800D

Bug ID	Description
365101	Fail IQC traffic test, all blocking at port8 for ip connection

FortiGate-1500D

Bug ID	Description
386683	Kernel panics after roughly 24 hours uptime
388646	FG-1500D: hardware test CPU/Memory test fail
370151	CPU doesn't remove dirty flag when returns session back to NP6
295041	Destination MAC address on NP6 offloaded IPv6 sessions are not updated when neighbor MAC changes

FortiGate-3810D

Bug ID	Description
375749	Sometimes NP6 gets `np6_fos_ipsec_sa_install 746 npu_tunnel_idx doesn't match` error message

AV

Bug ID	Description
373804	Encounter several scanunit daemon crash on US WiFi corp firewall.
384520	3600C crash on scanunit signal 11 (Segmentation fault)

Certification

Bug ID	Description
365586	Need to restart `fnbamd` to load import CRL.
373930	Unset ssh-certificate can not allow client to access with null password.

DLP

Bug ID	Description
369825	Do not compare DLP filesize filter for files inside an archive.

DNS Filter

Bug ID	Description
390957	Make DNS filter available under flow-inspection mode has been fixed.

FIPS-CC

Bug ID	Description
380703	Generation of IKE v2 nonces - NDcPP requirement.
375098	Remove CC error mode.
375102	Modify low level format for boot device (flash) in FIPS-CC mode.
375099	Update supported TLS cipher suites in FIPS-CC mode.
376860	IPSec ESP SA with stronger encryption than IKE SA shouldn't be allowed.

Bug ID	Description
387002	Add HMAC SHA-384/512 self-tests.
375100	Update supported SSH cipher suites in FIPS-CC mode.
387542	Remove CRL/Ceritifcate/CA may cause FIPS-CC self-test failure.
389003	FIPS-CC get self-test failure causes of `/etc/cert/ca/` changes, which causes system halt.
388181	Add support to break RNG health tests

Firewall

Bug ID	Description
376284	Fix CLI `firewall.addrgrp` when contain `url` upgrade from 5.2 to 5.4.
387367	Firewall is rebooting automatically.
373667	High vsd memory usage always triggers entering conserve mode when downloading file in SSL offload + IPS inspection.
368838	`active-flow-timeout` does not take effect for HTTP protocol when NP6 offloaded.
385983	`ssl-http-location-conversion` setting change from `enable` to `disable` by rebooting FortiGate.
375897	Sniffer policy upgrade from b0718 to b1064 failed.
383783	`policy64` and `policy46` ID should not use special id:4294967295.
297421	Fix policy re-push for multiple VDOMs.
297387 378560	On some platforms, UDP throughput is lower with more number of policies.

FOC

Bug ID	Description
382343	GTPV2 - Create Session response message denied due to 'ie-is-missing'

FortiCloud

Bug ID	Description
380506	FortiGate's `forticldd` daemon timer settings and updated timer discussion.

FortiLink

Bug ID	Description
379098	FortiLink Switch-Controller: Support "edge-port" setting for managed switch ports
380919	EAP tunnel is terminated at Authenticator(FGT) instead of at Auth-Server
387398	no admin password on Fortilink managed switch

FortiSwitch Controller

Bug ID	Description
388436	Traffic is intermittently blocked when HA FortiGate controls FSW by split interface.
387555	VLAN switch trunk function stops working

FortiView

Bug ID	Description
375394	Httpsd crashes when accessing page of Fortiview>VPN in GUI
390105	Fortiview VPN page shows minus value in field "Bytes(sent/received)" for L2TP and PPTP tunnels

FSSO

Bug ID	Description
386021	FSSO local poller fails on some X86 32 platform.

GUI

Bug ID	Description
371106	Removed trusted host is not re-indexed but replaced with 0.0.0.0/0.
371904	GUI does not prevent upgrading invalid CC signature image in FIPS mode.
375255	Cannot quarantine FortiClient device on FortiView because of javascript error from trunk 5-x.
288896	Should fall back to non-paging search if Oracle ODSEE 11.1 LDAP returns `LDAP_UNAVAILABLE_CRITICAL_EXTENSION`.
390088	Contract registration should accept characters.

Bug ID	Description
390794	Fix fail to create IPsec IKEv2 custom VPN tunnel with authmethod psk in GUI.
374221	SSLVPN setting portal mapping realm field misses the "/" option.
374339	SSLVPN setting page may not check the required fields.
386862	Large lists of address objects can take a considerable amount of time to load
292615	VLAN interface based on NPU vdom link can't be displayed in vdom-network-interface page
370360	VDOM read-only admin can view super admin and other higher priviledge admin's password hash via REST API and direct URL
373031	Unable to view FortiToken CD (FTK211) on FortiGate WebU
378817	Traffic Shapers list priority should display text word not number
391703	Add video links to FortiOS GUI
377539	Filter Overrides is removed after clicking on Apply on the Application Control profile

HA

Bug ID	Description
387212	HA gets out of sync frequently and hasync becomes zombie.
385999	Log backup of `execute backup disk xxx` feature does not work fine on HA master unit.
374418	No safe method for modifying secondary vcluster membership via the CLI.
266261	FortiExtender interface unable to get DHCP IP on a FortiGate in HA mode.
301101	`hasync` process is running 100% of CPU.
389192	Can't forward the SIP traffics(200OK messages) asymmetrical traffic environment in FGSP.
368447	FGSP should not sync static BFD setting.
375678	`update-all-session-timer` partially broken.
376449	FGSP: FGT1 clears SCTP Multihomed session marked established while data traffic is going through secondary path.

Bug ID	Description
378213	FGSP: after a reboot of the FortiGate that holds the SCTP secondary path, this session is missing and will be reopened.
390929	`hatalk` crashed when set `standaone-config-sync` from enable to disable.
376045	Software switch can't authorize FSWS successfully in HA scenario.
390926	After downgrade from b1086, HA can't be synced.
382364	Correct typo error in HA setting (change `helo-holddown` to `hello-holddown`).

IPS

Bug ID	Description
371254	ipsengine signal 11 crash happens on FG-60D/90D when IPS custom signature is detected.
378192	Per-IP shaper is not working for Application Category.
381547	Fix SynProxy offloading issue.
369137	IPSec performance decreased after upgraded FG-100D from V5.2.5 to V5.4.0 in certain test.
302853	Unnecessary debug message print out when change certain ips config.
379275	Fix FortiOS memory corruption caused by ips engine crash.
378252	Flow UTM: Save last session info into crash log when IPS engine crash happens.
379833	Adjust IPS CPU assignment to improve 3815D performance.
383525	Fix for IPsec mesh selectors not automatically brought up when phase2 auto-negotiate enabled.
379082	Proxyworker high CPU waiting for IPS to reinitialize.
389610	IPS app id/cat id should be datasrc and the cat id list source is inaccurate.
368729	State preservation test failed at max mem - attack packet not blocked
386050	WAD daemon consumes 99.8% CPU utilization
300785	Enabling sync-session-ttl will cause the existing IPS sessions to be removed
379084	Botnet DB update shouldn't cause IPS/AppCtrl signature reload in CMDB

Bug ID	Description
386271	After enabling IPS sensor with custom sig, in 60% chance need to wait for 30+ seconds to let ping packet pass
392520	Update IPS engine to build 3.294
392037	Traffic delays about 30 seconds after run `execute update-ips` command.

IPsecVPN

Bug ID	Description
376779	The algorithm names `sha384` and `sha512` are not displayed in the output of get commands for ipsec tunnel.
375749, 382568	Fix `TPE_SHAPER` drop on NP6 and an IPsec issue on FG-3810D.
383935	Policy-based routes does not work for Dialup IPSec routes in Fortios5.4.1.
376340	Change vpn ipsec phase1/phase1-interface peertype default from 'any' to 'peer'
388408	Incorrect output for "get vpn ipsec stats crypto"

Kernel

Bug ID	Description
385669	All FortiGate models crash with kernel panic

Log

Bug ID	Description
386446	`tunnelip` shouldn't be shown if no tunnel IP in the log.
376157	Logging performance improvement for IPS/AppCtrl.
284055	Improve the `antispam log fortiguardresp log` field.
377928	FortiCloud report can't be displayed on low-end platforms without SSD after burn image
373083	Broken remote log capabilities when resolve-ip is enabled

Router

Bug ID	Description
369864	BFD is DOWN randomly.
381974, 387318	Default static router setting should use `port1`.
382934	gpd may crash after executing `get router info bgp route-map`.
381908	Asymmetric routing in transparent VDOM has to be enabled for correct packet flow after upgrade from 5.2.
373820	Update `route_cache` only when there are changes in route table.
307530, 378075	Added support for BGP Local-AS feature.
391240	BGP UPDATES without NEXT_HOP
376765	E models cannot establish BGP session with Non-ARM platforms when MD5 password authentication enabled
391233	Multicast router doesn't send the PIM register after upgrading from 5.2.7 to 5.4.1

SSLVPN

Bug ID	Description
386167	Proxy vdom SSLVPN IPv6 av doesn't block virus if IPv4 policy UTM disable.
381112	Website drop-down menu does not work when accessed via SSLVPN bookmark.
371933	Unable to connect to SMB server which supports only NTLMv2.
371597	SSLVPN fail to login FGT 5.4 bookmark through Fortinet bar with `url-obscuration` enable.
371551	Fix SSLVPN user authenticates doesn't follow firewall policy order when change user group order until reboot.
371807	Try next server when LDAP group auth failed on first firewall policy.
377207	fix could not access `owncloud` properly through SSLVPN.
377557	Change tunnel set-up timeout threshold for SSLVPN web portal with `limit-user-logins`.
382586	Fixed `path not found` is printed out when certificate is changed.

Bug ID	Description
384200	Fix SSLVPN tunnel sometimes gets disconnected without error message.
374859	Fix got fork() failed after SSLVPN enter conserve mode.
379450	Fix SSLVPN crash with segmentation fault in `sslvpn_ap_table_get` after upgrading to 5.4.1.
379076	RDP session will be disconnected after the `idle-timeout` is expired on web-portal.
378103	Fix SSLVPN/newcli crash when running `get vpn ssl monitor` if there are more than 10000 tunnels.
380201 382393	Fixed SSLVPN has high CPU/crashed.
375561	`RESOURCE_LEAK` found in SSLVPN.
386968	Getting error `Failed, suspended by other users` when edit some content using Firefox.
379076	RDP session will be disconnected after the `idle-timeout` is expired on web-portal.
382828	SSLVPN web-mode not displaying login page of internal server, but tunnel-mode is OK.
355913	SSLVPN setting -> edit authentication/portal mapping page issue
387966	Username replaced by peer name in certificate based SSLVPN
375379	Username and password are displayed in clear text in the browser bar for CIFS/SMB SSL VPN Bookmark

System

Bug ID	Description
369540	Kills the parent process (fgfmsd) and causes script `exec reboot` from FMG does not work on FortiGate.
372629	Hardware issue of FG-60D causes config to be lost.
375188	After factoryreset2, split port interfaces are lost.
375141	When NP6 offload is enabled, traffic will show up in wrong VDOM but correct VLAN interface.
380157	ZebOS issues on new VDOM.

Bug ID	Description
385362	Remove username and password requirement for CLI `exec central-mgmt register-device FMGSN KEY username password`.
367471	Fragmented out-of-sequence ICMP Reply can loop endlessly in npu-vlink.
385455	Inconsistent trustedhost behavior.
381857	LACP passive mode voluntarily initiate LACP negotiation then aggregate interfaces unexpected establishing.
374481	Alertmail does not work on CHANGED management VDOM.
384698	Cache memory increased abruptly.
390570	FEXT discovery issue fixed.
390592	Update geoip database to version 1.057.
387675	ARP-Reply packets drops in NP6.
376452 385278	ICMP packets with HBH options are now forwarded properly.
389194	End of Daylight Savings (DST) timezone Turkey/Istanbul GMT +3.
371387	Add two trailers for FK images, to make it pass the upgrade test.
381675	Support SNMP query for individual CPU Core monitoring in kernel-3.2.
390207	Fix ixgbevf driver VLAN issue.
292237	FG-200D hangs with transmit timeouts.
378761	Allow local-in traffic When system memory reaches 94%.
378558 380653	LACP over Virtual Wire Pair on 800C, ports not forwarding LACPDUs.
372632	Eliminate kernel crash and reboots while FortiManager pushes config changes.
356245	Fix LACP ignoring peer ID change.
380161	No reply to SNMP queries if reply should be routed via PBR.
374715	Add TCP seqnum verification to BGP on RST packets.
302021	Enable FortiTest feature for 400D/600D platforms.

Bug ID	Description
378825 385964	Enable diagnose hardware test on FG-100D/800D and fix related bugs.
389047	Unable to edit/create system interface when a large number of detected devices exist has been fixed.
370778	Connection problem to new master FQDN address of FMG after failover.
386478	Add LFG60C B0735 (LENC) device failed with internal error.
375338	FortiManager with *super_admin* profile install capture-packet meet privilege issue.
373344	"diag ip address list" still show ip address although dhcp lease time expired
376144	FMG failed to change FGT HA slave to master
380600	CLI configurable NP6 optimization
388603	after reassembly fragmented UDP packet, the s/d port become 0
365441	FGT is showing capwap IP (224.0.1.140) and mac-address (01:00:5e:00:01:8c) even no capwap enable on the port
369353	Destination MAC address will not be updated for NPU offloaded IPv4 sessions sometimes.

Tablesize

Bug ID	Description
382232	FG-900D explicit proxy max users < FG-800D.
390053	Increase firewall.schedule limits on higher end

Upgrade

Bug ID	Description
393056	Explicit proxy config lost on interfaces after upgrading if vdom is enabled

Visibility

Bug ID	Description
365259	src-vis crash on device with device detection eanbled on one-arm-sniffer interface

VM

Bug ID	Description
372030	Increase VM00 memory limit to 1.5G.
376567	Fix network reachability issue of AWS instance launched from customer created ami.
372040	VLAN not forward traffic out on non-root VDOM.
374905	Error when attempting to deploy vApp on ESXi v6.0.0.
372487	Fix FG-VM stuck at rebooting the system when its rebooting.
378482	TCP/UDP traffic failing when NAT/UTM is enabled on FG-VM in KVM.
369167 391519	Improve `cloudinit` boot up config sequence.
371982	Fix FG-VM have no `gui-wanopt`.
392654	IPv6 basic network settings not available on unlicense VM01 or higher

VOIP

Bug ID	Description
370201	Fix the `imd` crash issue when unregistering SIP with asterisk (*) contact, or multiple `REGISTER` message with same AOR and multiple contacts.
382315	Fix the issue that SIP re-invites causing excessive memory consumption in VOIPD.

WANOPT

Bug ID	Description
373825 376035	Fix Traffic was broken over A-P mode WANOPT on first attempt after WAD restarted.
393114	WAD crash in wad_str_copy_str after upgrade to 5.4.1

Web Application Firewall

Bug ID	Description
378194	Suspect WAF breaks JSON file by adding zero to the end.
383520	WAF url-access not work.

Web Filter

Bug ID	Description
378234	WAD crash in `wad_fmem_free` after upgrade to 5.4.1.
388731	Fix `rpc-over-http` will cause WAD crash when enable UUID is not found in RTS.
382501	Kerberos authentication fails with `unexpected token length` error.
376486	WAD not supporting full webfilter with transparent policy and external webproxy in SSL deepscan mode.
373251	Local FortiGuard overrided rating sometimes doesn't work well.
380119	Webfilter Static URL filter blocking domains with similar name.
377206	Fix wanopt log incorrect and wad ntlm auth crash.
390446	Fix webfilter urlfilter mismatch.
380324 380682	Fix proxyd and wad ssl related issues.
388957	Fix YouTube EDU filter: None, Moderate, Strict.
393381	Suggest add webfilter profile fgd block and override config CLI correlation check

WebProxy

Bug ID	Description
384581	Explicit Proxy Signing Certificate for replacement pages resets to default.
374706	Fix a memory leak on `proxyd`.
380324	Transparent Proxy SSL Inspection closes connections before completion of SSL negotiation and/or complains of `Bad Record`.
389059	Improve SOCKS debug and WAF&AV scan on HTTP request.
381429	CP8 does not work for Proxy SSL acceleration.
378518	Fix WAD will crash when using web-proxy profile to add/remove HTTP headers.
390124 391748	Fix WAD SSL session ticket will cause crash on hello request, and add cert status extension support to fts.
371991	`YouTube_Video.Play` is not recognized with HTTPS in Application control Override.

WiFi

Bug ID	Description
387163	Fix WiFi driver crash for 3.2 kernel FWF platforms.
371374	Add back support of wave2 FAP421E/423E.
376921	FortiGate kills `cw_acd` daemon continuously in 900+ APs large setup.
365255, 381030	WPA-Personal passphrase should support a fixed-length of 64 hexadecimal digits.
387163	Fix WiFi driver crash for 3.2 kernel FWF platforms.
309597	Fix WiFi region codes and DFS support.
374617	Memory leak happens when change large WTP sessions's security option.
370657	FDS daemon should return error code when fortiap version is not available in FAPV
374385	Fortinet_WiFi is not signed by PositiveSSL_CA/Fortinet_WiFi_CA after LENC license is loaded
387163	FWF30E / kernel error happpened when purge vap interface by CLI

Common Vulnerabilities and Exposures

Bug ID	Description
379870	FortiOS 5.4.2 is no longer vulnerable to the following CVE References: • 2003-1418 • 2007-6750 Visit https://fortiguard.com/psirt for more information.
373707	FortiOS 5.4.2 is no longer vulnerable to the following CVE Reference: • 2016-1550 Visit https://fortiguard.com/psirt for more information.
383538	FortiOS 5.4.2 is no longer vulnerable to the following CVE References: • 2016-3713 • 2016-5829 Visit https://fortiguard.com/psirt for more information.
381168	FortiOS 5.4.2 is no longer vulnerable to the following CVE Reference: • 2004-0230 Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
378697	FortiOS 5.4.2 is no longer vulnerable to the following CVE Reference: • 2016-2512 Visit https://fortiguard.com/psirt for more information.
383564	FortiOS 5.4.2 is no longer vulnerable to the following CVE Reference: • 2016-5696 Visit https://fortiguard.com/psirt for more information.
389610	FortiOS 5.4.2 is no longer vulnerable to the following CVE References: • 2016-6309 • 2016-7052 Visit https://fortiguard.com/psirt for more information.
367040	FortiOS 5.4.2 is no longer vulnerable to the following CVE Reference: • 2016-7541 Visit https://fortiguard.com/psirt for more information.
389206	FortiOS 5.4.2 is no longer vulnerable to the following CVE References: • 2016-2177 • 2016-2178 • 2016-2179 • 2016-2180 • 2016-2181 • 2016-2182 • 2016-2183 • 2016-6302 • 2016-6303 • 2016-6304 • 2016-6306 Visit https://fortiguard.com/psirt for more information.
370360	FortiOS 5.4.2 is no longer vulnerable to the following CVE Reference: • 2016-7542 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.4.2. 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)

DLP

Bug ID	Description
393649	Executable files may not be blocked by DLP built-in `exe` file-type filter.
379911	DLP filter order is not applied on encrypted files.

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.
391537	Buffer size is too small when sending a large vulnerability list to FortiGate.

FIPS-CC

Bug ID	Description
375149	NDcPP requires a SSH server rekey.

Firewall

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.
364589	LB VIP slow access when cookie persistence is enabled.

FortiGate-3815D

Bug ID	Description
385860	FG-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

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

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 my display the incorrect drill down *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.

Bug ID	Description
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 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`.
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.

Bug ID	Description
375290	Fortinet Bar may not be displayed properly.
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 re-direct 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.
374221	SS LVPN 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 it 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.

Bug ID	Description
374183	*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.
393267	Not possible to edit existing Web Filter profile.
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.

HA

Bug ID	Description
391084	HA unable to sync inversed object entries.
388044	Four member HA Cluster do not always re-converge properly when HB links are re-established.

IPS

Bug ID	Description
393675	SSH due to Application Control Proxy in the Security Profile.
393958	Shellshock attack succeeds when FGT is configured with `server-cert-mode replace` and an attacker uses `rsa_3des_sha`.
394157	IPS archive not uploaded to FAZ when it is in realtime mode.

IPSec

Bug ID	Description
375020	IPsec tunnel Fortinet bar may not be displayed 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.

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.
391786	`Logdiskless` FGT does not generate a log indicating a sandboxing result.
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.

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 Fortinetbar may not be displayed.

Bug ID	Description
393698	SSL VPN web mode `http/https` SSO will keep trying even if the password is wrong.
307465	Fail to Copy & Paste through RDP when connected by SSL VPN web mode.
393943	SSL VPN crash when connect to win2008 smb/CIFS bookmark with wrong password.

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 can not use `ssh-dss` algorithm to login 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.
388046	`Confsyncd` memory leak.
393395	The role of new VAP interface should be set as LAN.
393042	IPv6 traffic not distributed according to the `lacp L4` algorithm.
393343	Remove botnet filter option if interface role is set to LAN.
392960	FOS support for V4 BIOS.
392125	FGT to FMG backup config returned with the *Management server is not configured* error message.
392125	After an HA failover some of the multicast streams stop.

Upgrade

Bug ID	Description
269799	sniffer config may be lost after upgrade.
289491	When upgrading from 5.2.x to 5.4.2, port-pair configuration may be lost if the `port-pair` name exceeds 12 characters.
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.

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.
378421	Committing any change on SSL VPN Settings over web page returns `error:500`.

Web Filter

Bug ID	Description
394515	URL exempt/allow does not work as expected when certificate-inspection is used.

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