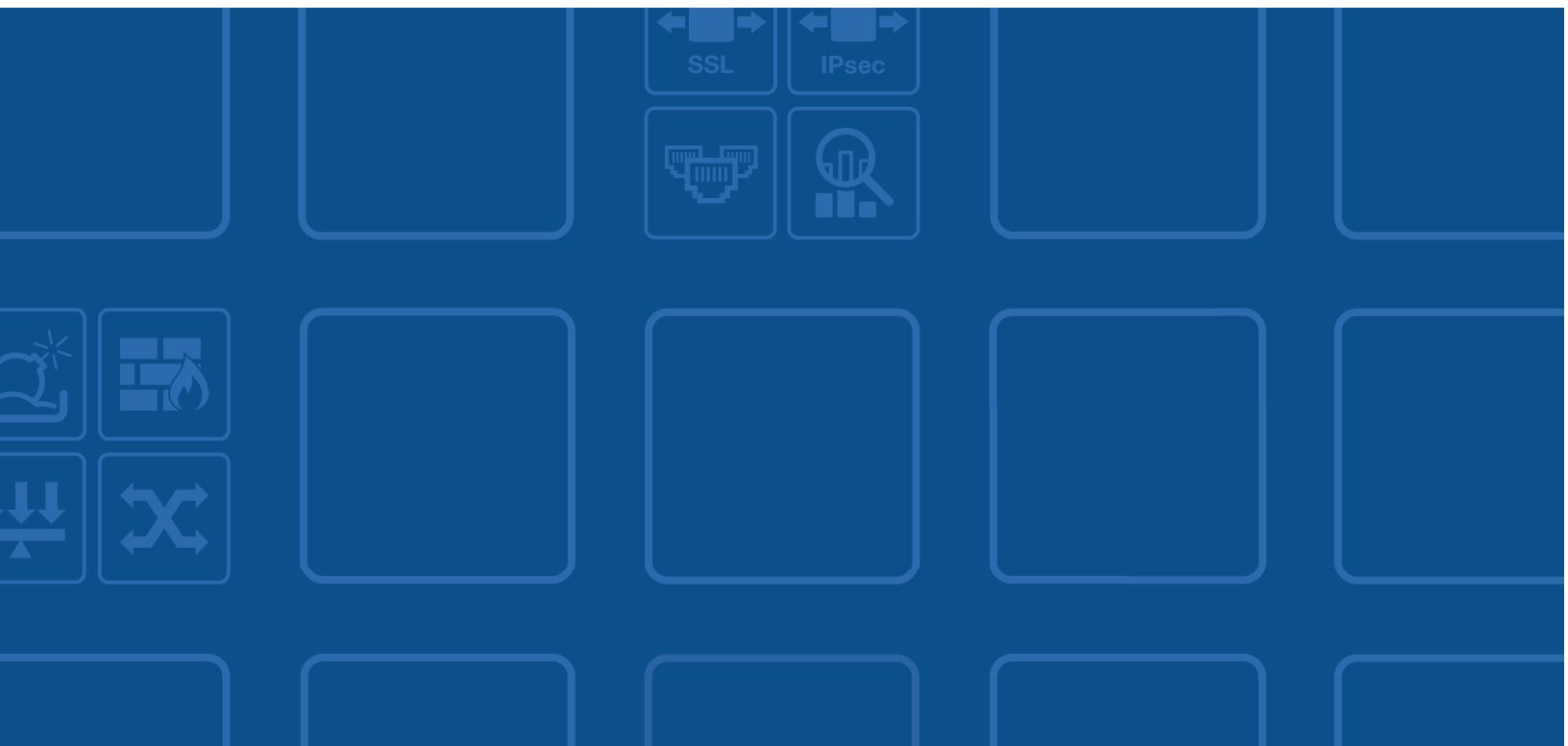
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.4.1



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 5.4.1 Release Notes

01-541-370115-20171110

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-06-08	Initial release.
2016-06-09	Moved 373739 from Known Issues to Resolved Issues. Added FOS-VM64, and FOS-VM64-KVM to Supported Models. Added *FortiGate and FortiWiFi-92D Hardware Limitation* section to Special Notices. Added *FortiClient Support* to Special Notices.
2016-06-10	Removed 306486 from Resolved Issues. Added 370337 to Resolved Issues. Added *FortiClient Profile Changes* section to Special Notices.
2016-06-15	Added *Model 60D Boot Issue* section to Upgrade Information. Added 373127 to Known Issues. Related to this bug, added *FG-80D and VLAN Interfaces* section to Special Notices.
2016-06-16	Added *FortiClient Profiles* section to Upgrade Information.
2016-06-17	Added 304566 to Resolved Issues.
2016-06-21	Added FGT-60D, FWF-60D, FGT-60D-POE, FWF-60D-POE, FGT-80D to Supported Models. They are released on build 5447.
2016-06-22	Updated *Upgrade Information > Model-60D Boot Issue* section. Removed *FG-80D and VLAN Interfaces* from Special Notices since 373127 has been fixed. Added 373127 to Resolved Issues.
2016-07-05	Updated Product and Integration Support Added *Special Notices > Removed SSL/HTTPS/SMTPS/IMAPS/POP3* section
2016-07-08	Updated Upgrade *Information > Upgrade Paths URL*.
2016-07-11	Added *Special Notices > FortiClient (Mac OS X) SSL VPN Requirements*.
2016-07-14	Added 369659 to Resolved Issues.
2016-07-15	Added FG-60E, FG-61E, FWF-60E, and FWF-61E to Supported Models.
2016-07-27	Added a note to *Special Notices > FortiClient Profile Changes*.
2016-08-02	Added licensing information to *Special Notices > FortiClient Support*.

Date	Change Description
2016-08-04	Added *Upgrade Information > Amazon AWS Enhanced Networking Compatibility Issue*.
2016-08-11	Added *Product Integration & Support > VM-Series - SR-IOV*.
2016-08-19	Updated *Supported Models > FG-60E and FG-61E* to build 5577.
2016-08-25	Updated *Supported Models > FWF-60E and FWF-61E* to build 5578. Added *FortiGate-60E/61E and FortiWiFi-60E/61E* section to Resolved Issues.
2016-08-30	Added 385860 to *Known Issues > FortiGate-3815D*.
2016-09-12	Added FG-2000E and FG-2500E to Supported Models.
2016-09-28	Added information to the FortiAP section in *Product Integration and Support > FortiOS 5.4.1 Support*.
2016-10-24	Added 295508 to *Resolved Issues > System*.
2016-11-02	Added FG-90E, FG-91E, FG-100E, FG-101E, FG-200E, FG-201E and FWF-50E-2R to *Supported Models*.
2016-12-05	Updated *Supported Models > FG-1500D and FG-3700D* to build 7386.
2017-01-25	Added 289491 to *Known Issues > Upgrade* section.
2017-02-14	Updated Upgrade section to include 5.2.8.
2017-02-16	Updated *Special Notices > FortiGate units managed by FortiManager 5.0 or 5.2*.
2017-03-03	Added 290229 to *Resolved Issues > System*.
2017-11-10	Added 273973 to *Known Issues > Upgrade*.

Introduction

This document provides the following information for FortiOS 5.4.1 build 1064:

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

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.4.1 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30D-POE, FG-50E, FG-51E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-90D, FGT-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-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700DX, FG-3810D, FG-3815D, FG-5001C, FG-5001D
FortiWiFi	FWF-30D, FWF-30E, FWF-30D-POE, FWF-50E, FWF-51E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
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 5.4.1 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 5.4.1. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays the build number.

FG-52E	is released on build 5416.
FG-60D	is released on build 5447.
FG-60D-POE	is released on build 5447.
FG-1500D	is released on build 7386.
FG-3700D	is released on build 7386.
FG-60E	is released on build 5577.
FG-61E	is released on build 5577.
FG-80D	is released on build 5447.
FG-90E	is released on build 5735.
FG-91E	is released on build 5735.
FG-100E	is released on build 5654.
FG-101E	is released on build 5654.
FG-200E	is released on build 5706.
FG-201E	is released on build 5706.
FG-2000E	is released on build 5632.
FG-2500E	is released on build 5632.
FGR-30D	is released on build 5413.
FGR-30D-A	is released on build 5413.
FGR-35D	is released on build 5413.
FWF-50E-2R	is released on build 5631.
FWF-60D	is released on build 5447.
FWF-60D-POE	is released on build 5447.
FWF-60E	is released on build 5578.
FWF-61E	is released on build 5578.

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 1064.

What's new in FortiOS 5.4.1

For a more detailed list of new features and enhancements that have been made in FortiOS 5.4.1, see the *What's New for FortiOS*5.4.1document available in the Fortinet Document Library.

Security Fabric

Logical View

A topology diagram reflects the logical representation of the network. This includes:

- How the fabric is formed (which interfaces connect to each FortiGate)
- Which devices are connected to each segment (LAN interface)
- Traffic bandwidth originating from each segment

Physical View

A topology diagram reflects the physical topology of the Security Fabric. This includes:

- How the fabric is formed
- All FortiGates, FortiSwitches and endpoints (hosts) in the network
- Relative traffic volume based on bandwidth, packets, sessions, etc. behind each FortiGate

Endpoint Telemetry

Enhancements to the FortiClient Security Profile to integrate with the Security Fabric:

- Utilize endpoint discovery and registration to extend visibility beyond the firewall
- Obtain user identity and endpoint security context (vulnerability, security posture, OS details, interface, IP address, MAC address)
- Modular client with cross platform support

Learning Mode & Report

Learning Mode is a new Firewall Policy option, similar to the Allow Policy, with fully enabled logging capabilities. All logs generated from these policies will be tagged as *Learning*.

A new Cyber Threat Assessment Report is also available. It uses all of the Learning Logs, across all traffic and security vectors, to generate a complete summary report. This enables users to easily implement a "monitor then enforce" process.

FortiView

Cord Chart

A visual representation of pairs of networks (interfaces) that are connected to each other in relation to other networks. It provides a top-level view of how flows are traversing your network.

Web Search Phrases

Extension of FortiView to analyze web search phrases in the network.

Cloud Application Security Enhancements

Enhancements include:

- Extensions to the cloud application UI and database
- Enable fine-grained control over each cloud service (Allow, Block and Monitor commands)
- Block individual commands (File Upload/Download, User Login etc.)

FortiSwitch Controller

Several large extensions have been added to FortiSwitch Controller to support all new generation FortiSwitch models. Extensions include:

- Simplify the process to dedicate a FortiGate interface, or aggregate, to a FortiSwitch connection
- Consolidation of VLAN objects to reuse the same VLAN objects and configuration process on interface or switches
- Support different FortiSwitch topologies, including Single-Tier, 2-Tier, Ring, etc.
- Support aggregate and redundant links within topologies

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 or later is supported with FortiOS 5.4.1. Upgrade managed FortiClients to 5.4.1 before upgrading the FortiGate to 5.4.1.

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. 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. A new license will need to be procured for either FortiClient EMS or the FortiGate. To verify if a license purchase is 5.4.1 compatible, 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 5.4.1, 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, the FortiClient provisioning capability will no longer be available in FortiClient profiles on FortiGate. FortiGate will be used for end-point 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.

Upgrade Information

Upgrading to FortiOS 5.4.1

FortiOS version 5.4.1 officially supports upgrading from versions 5.2.7, 5.2.8, and 5.4.0.

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 greatly increases the interoperability between other Fortinet products. This includes:

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

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 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

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

Model-60D Boot Issue

The following 60D models have an issue upon upgrading to FortiOS 5.4.1. The second disk (flash) is unformatted and results in the /var/log/ directory being mounted to an incorrect partition used exclusively for storing the firmware image and booting.

- FG-60D-POE
- FG-60D
- FWF-60D-POE
- FWF-60D

To fix the problem:

If your FortiGate device is currently running FortiOS 5.2.7:

1. Backup your configuration.
2. Upgrade to 5.4.1 B5447.

If your FortiGate device is currently running FortiOS 5.4.0 or 5.4.1:

1. Backup your configuration.
2. Connect to the console port of the FortiGate device.
3. Reboot the system and enter the BIOS menu.
4. Burn the firmware image to the primary boot device.
5. Once the system finishes rebooting, restore your configuration.

FortiClient Profiles

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

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

- Advanced FortiClient profiles (XML configuration)
- Advanced configuration, such as configuring CA certificates, unregister option, FortiManager updates, dashboard Banner, client-based logging when on-net, and Single Sign-on Mobility Agent
- VPN provisioning
- Advanced AntiVirus settings, such as Scheduled Scan, Scan with FortiSandbox, and Excluded Paths
- Client-side web filtering when on-net
- iOS and Android configuration by using the FortiOS GUI

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

Unified Disk Usage

FortiOS 5.4.1 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 5.4.1.

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 5.4.1, 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 this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.4.1 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 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 5.4.1 support

The following table lists 5.4.1 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 • 5.2.3 and later
FortiClient Android and FortiClient VPN Android	• 5.2.9 • 5.2.6 and later

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-421E and FortiAP-423E platforms only**: Please call customer support for the FortiGate WiFi Controller image to manage these FortiAP models.
FortiAP-S	• 5.4.2
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	• 3.279
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 5.4.1. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
278240	100% CPU usage when system is idle; signal 14 occurs.
302818	FortiSandbox analytic verdict not logged in UTM log.
368258	Fix upload chunked scan and learn file name from URL in decoded format.

Certification

Bug ID	Description
366274	Request an update on the country code in CSR.
306645	Cannot use `SCEP(https)` to load the `subCA` certificate.
301574	MSCHAP RADIUS VSAs are packed in the same AVP.
288440	Status of expired CA certificate in Certificate GUI is still valid.

DLP

Bug ID	Description
277594	Proxyworker stops working when using IMAPS or POP3 servers for email.
365320	Files and file names are incorrectly identified in a MIME message.
175146	When SMTP protocol checks for the `flag local-override`; they were missing in several places.
369307	Remove fake file names when DLP file names matches.

Firewall

Bug ID	Description
304317, 304136	WAD daemon may crash when enabling WAD debug.
304432	Protect server does not work when enabling the Proxy AV and deep inspection.
300491	User can accidentally delete/change policies configured from the GUI using Policy ID command `gui-advanced-policy enable`.
368191	FTP-Active session does not work when the `session-helper` does not translate the FTP PORT information.
357522	Improve the multicast policy handling in NAT mode.
365937	Browser does not load objects if the VS persistence is set to `http-cookie`.
294263	Traffic log reports the wrong service for dropped traffic.
303962	VIP IP unexpectedly responds to `fgfm` requests.
304566	Fix proxyworker crash when `ssl inspect-all` is set to `deep-inspection`.
369659	Using the DNAT + TNS session-helper, FGT produces the incorrect `Seq#` translation.

FortiGate-60E/61E and FortiWiFi-60E/61E

Bug ID	Description
378711	VPN IPsec concentrator traffic fails to pass FGT.
377112	FWF-61E loses VAP settings upon upgrade.
377829	Dialup IPsec VPN fails to pass traffic and the FGT-60E/61E stops working when trying to reboot.
382683	Error messages are displayed when performing a memory test on FGT-60E.
382704	Error messages are displayed when doing a warm reboot after a memory test.
382400	Error messages are displayed on console when running `diag hardware deviceinfo nic`.
377999	Shapers (`traffic shaper or per-ip shaper`) fail for NAT64/46 if traffic is off-loaded to NP6lite.

FortiGate-80D

Bug ID	Description
373127	FG-80D VLAN interfaces may fail to pass traffic.

FortiGate-92D

Bug ID	Description
298348	IPv6 does not work on the internal interface.

FortiGate-500D

Bug ID	Description
296025	FG-500D reboots after a kernel panic.
274870	Optical SFP module compatibility does not work as expected.

FortiGate-1500D

Bug ID	Description
368642	System stops working randomly a couple of times a day.

FortiGate-5001C

Bug ID	Description
246417	FG-5001C becomes unresponsive.

FortiSwitch

Bug ID	Description
303818	Allow user to specify `All defined VLAN` to be `allowed vlan` on FortiSwitch ports.

FortiView

Bug ID	Description
301315	In the Device Topology page, a dependency warning should appear if no interface has device detection enabled.
303787	*Application page* > *Filter on a Unknown Application* does not work.

Bug ID	Description
303823	*Policy* > *Source and Destination Interface* displays an `unknown-0` message.
300055	In the *Traffic Shaping* page , bandwidth and dropped bytes are not accurately listed for the *Forward Shaper*.
299900	In the *Traffic shaping page*, the IPv6 shaping misses the `reply-shaper name` and is not able to drill down the menu.
304068	Create a FortiFone device group and FortiCam device group.
294632	Users are not able to customize how quickly it will to scan an active device.
308676	Change the NST terminology.
303747	*Source* > *Filter Source Device* does not work.
277558	*Policy page* > *IPv6 policy* is displayed as IPv4 policy in realtime view.

FortiWiFi-60D

Bug ID	Description
306121	FWF60D kernel panic occurs after upgrading to v5.4.

FSSO

Bug ID	Description
302908	`Smbcd` continuously requests for memory; this causes the system to enter conserve mode.
307920	`authd` is inserted in two non-portrange entries into `fsso list` with the same IP address.

GUI

Bug ID	Description
303642	Route lookup window is empty.
303645	If no route is found, the IPv6 route lookup result is not accurate.
302576	GUI displays the password-policy rules on the Admin page even when the password policy does not apply to that admin user.
303038	*Dead Peer Detection* setting in the *IPsec Tunnel Templates* page shows *On-demand* instead of *Enable*.

Bug ID	Description
303776	Options are not available in the Log View; a JS error occurs when setting a filter in the protocol field.
304100	Users are not able to enable *Feature Select* in Global or VDOM on the following platforms: FG-3700D, FG-3700DX, FG-3810D and FG-5001D.
304119	*Explicit Proxy Policy* receives an internal error if *All Ports* is enabled in any of `ssl-ssh certificates` in the Inspection Profile.
283656	NP6 offloading is lost when the IPsec interface has the `aes256gcm` proposal enabled.
304491	Users are not able to set the *IPsec VPN Xauth User Group* to inherit groups from the policy in the GUI.
304495	In the *Network* > *Explicit Proxy* page, when users edit *Listen on Interfaces*, the page stops responding.
304395	The *SSLVPN Web Portal RSA Token* in *New Pin Mode* does not work.
304645	Traffic Shapers bandwidth unit displays in kb/s while the backend config is displayed mbps/gbps.
304627	If you try to restore the config in the GUI, only master's config is restored, the slave's config is not restored.
304436	GUI might show a different received/sent value in CLI compared to the *GUI >Modem* monitor page.
304439	Users are not able to set UTM profiles in the IPsec Action Policy page.
304455	*GUI* > *Interface* > *DHCP Server* > *Advanced* > *DHCP Client List* page does not correctly display on Chrome 47.
307182	*GUI* > *Firewall* > the color setting for the firewall address group resets to default while doing any changes to `addrgrp`.
310993	Add a *Feature Store* button for on-net/off-net features, but disable by default.
295912	FortiAnalyzer displays as disconnected in the *Unit Operation* widget even though it is connected.
295628	*Loading Application* sensor does not work with custom Admin Profiles.
308104, 308105	Improved Enterprise Bundle object visibility.
296342	FortiClient monitor display improvements.

Bug ID	Description
305817	URL category within *Explicit Proxy Address Objects* are not shown in the GUI.
260301	Do not allow Wanopt to be enabled unless the peer is configured.
300372 -	GUI stops working when the Admin tries to login with two factor authentication mail token.
303576	Add a *Feature Store* button to allow user the put multiple interfaces (and ANY) into a policy.
306393	Removes the lines to Fortilink ports on the faceplate.
354331	Fix incorrect validation for quarantine duration.
369359	Cannot create or update recurring a schedule from the GUI.
277780, 269479	Update *receive timeout* to prevent connections from blocking access to the GUI access.
308695	GUI Updates for Additional DHCP Options table.
369172	GUI change resets VIP custom color configuration to default.
285156	GUI shows duplicate IP address and interface name in the FortiClient monitor page and the Device list page.

High Availability

Bug ID	Description
304433	New import local certificate causes the HA to become out of sync in a Multi VDOM environment.
365661	Some TCP session can not be synced with master on a slave unit.
366745	FortiCloud can not be activated via the HA GUI.
357298	After a policy installation, `session hardware off-load` does not work as expected.
307013	`hasync crash signal 11 (FGSP)` occurs in `stand-alone-config-sync`.
302687	`ha-mgmt-interface IP address` is not assigned after rebooting.
289516	RTP pinholes are deleted after some time on the slave unit.
286827	BGP MD5 authentication error occurs after a HA failover.
356239	HA HeartBeat is down when using the following command: `restore vdom config`.

Bug ID	Description
371446, 270267	Slave/Passive unit in HA virtual cluster generates traffic logs for failed traffic.
365669	FGSP cannot establish `session-helper` protocols in an asymmetrical traffic environment.

IPS

Bug ID	Description
306277	Flow-based local URL filter does not work on FGT-3700D/FGT-1500D.
364309	`ipsufd` does not work as expected in a HA failover.
309844	`NTUrbo mbuf` error occurs because tx packets are not handled properly. Correct a typo which causes the unnecessary checksum updates for each packet.
308064	Performance improvement for NTurbo IPS on FG-3000D and FG-600D
306713	`NTurbo local mbuf` handling problems when processing IP fragmented packets.
307443	Fragment IPv6 packet triggers a bad IP header log.
299585	IPS engines remained 99.9% busy due to production traffic.
306648	The Virtual Wire default configuration should use `certificate-inspection` as the `ssl-ssh-profile`.

IPsec

Bug ID	Description
296439	L2TP over IPsec tunnel cannot be established.
304740	The IMD memory leak occurs when the package is retransmitted.
365288	IPsec tunnels do not appear if zones are used in `policy src` and `dst`.
303584	Multiple IPSec Tunnels will occasionally print out `FIXME np6_fos_check_ipsec_offload:1297`.
307794	`unregister_netdevice` error message appears and the unit enters an unstable state.
295591	The ESP sequence number is invalid after lag interface member is disconnected then reconnected.

Log & Report

Bug ID	Description
304217	`miglogd` stops working; its protocol and port overlaps with another service.
304533	AntiVirus log does not have a URL section when a Gmail attachment is downloaded.
302728	Omit specific log messages or give them lower severity level.
301401	Local Report is generated even if it is disabled.
306691	URL in Web Filter UTM logs is truncated When the `log-all-url` option is enabled in the Web Filter Profile.

Modem

Bug ID	Description
304965	NTT LTE modem UX302NC does not detect dialtone correctly.

Proxy

Bug ID	Description
372706	Improve Proxyworker handling for propagating the *abort close* signal.

Routing

Bug ID	Description
354463, 368257	Disconnected link causes high CPU usage and `lnkmtd` stops working in measured-volume mode.
357487	`pim-sm bsr flooding` is heavy on FortiGate.
306321	Interface is mandatory when creating a GRE tunnel.
306331	Copy DSCP value from inner to outer header in the GRE tunnel.
354454	Policy routing table is not updated when the WAN interface is disconnected.
309128	The default route is duplicated in FIB.
354463	Link-monitor's fail times are not accurate.

SSL VPN

Bug ID	Description
300054	When upgrading from 5.2, the SSL VPN login replacement message is reset to the factory default.
310928	Pages Linked from within SSL VPN Portal do not render correctly.
303866	Unable to access web pages when use the FortiClient for iPad.
306982	The `auth` policy is ignored if the specified user is a member of group.
310566	SSL VPN Web Mode login times out in 5 minutes even if it is not idle.
276730	When split-tunneling is set to a non default value, it is not shown in the config.
290869	SSL VPN `.xls` attachments downloaded from bookmark page are corrupted.
301160	Web application does not load when using SSL VPN web access.
364918	Should not add `SSLVPN_TUNNEL_ADDR1` to TP mode in VDOMs when the system reboots.
307012	SSL VPN is unable to connect in tunnel mode, multiple stale sessions occur for same user.
306020	Three `sslvpnd` processes leaking (radius remote authentication context).
300748	MS Remote App and Desktop Connections are not shown via the SSL VPN web portal.
302596	SSL VPN web portal RDP/VNC does not connect.

System

Bug ID	Description
301947	On NP6 ports, hairpinned traffic is blocked after the traffic that initialized the original NATs stops responding.
303626	Switch VLAN is not accessible in trunk (LACP) mode on 200 series platforms.
297923	Newly created HW switch on NP4 platforms is not accessible until users reboot.
304118	VLAN and hardware switch interface loses the secondary IP during the upgrade from v5.2 to v5.4.
303906	The CLI stops working when configuring Interface Policy6.
304472	Health-check over PPPOE interface does not work after a FGT reboot.

Bug ID	Description
304320	LENC FGT is not able to update the `modem-list` and `message-update`; it is notable to connect to FortiAnalyzer.
303959	When the VDOM is enabled, the `EAP_proxy` is not able to handle the certificate chain with a depth of more than two.
304667	When FGT has only one disk and it is used by WANopt, the factory reset does not reset the disk to log.
305058	FortiGate encounters a system hang issue caused by the `dialup ipsec vpn`. The `unregister_netdevice` error message appears.
307675, 310201, 307299	Split port was mapped to the wrong VDOM and traffic could not go through.
363356	Change SNMP counters `fgVpnTunEntInOctets/fgVpnTunEntOutOctets` from 32bit to 64bit.
294859	`dmz1 interface status` is down on some units.
310071	Specific SFP shared ports LED (Port18 on FG-1000C) is not lit properly.
309821	ICMPv6 packets with *Hop-by-Hop Options* are not decoded properly by the built in sniffer.
256614	Admin server key is accessible via `print-file/gzfile`.
310686	Admin status is down in the Fail Detect feature on the 40G interface.
302272	`medium_type` is incorrect on shared ports.
301702	Fragmented packets are not forwarded in transparent mode.
273848	License Status did not differentiate between `low-crypto-license` and LENC license.
301842	NP6 PBA Leak occurred.
307342	Extend DHCP Option Support to 8 Fields.
309452	`diag` command could give *read-only* admins certain elevated privileges.
300249	Alert Email are sent out with the wrong time interval.
371660	FortiManager is unable to set `uninterruptible-upgrade` settings on the FortiGate.
370951	FortiCloud activation fails if traffic is sourced from an interface other than the default route path.

Bug ID	Description
371104	Allow reply packet to pass if `asymroute` is enabled.
368459	Ensure 802.3ad and LACP does not send traffic to down port.
295508	PPPoE connection is unstable and cannot recover automatically.
290229	Read-Write and Read-Only administrator profile accounts see an invalid navigation panel after login.

Tablesize

Bug ID	Description
367574	*Firewall* > *Increase Firewall Policy* to 200,000 for FG-3000 series and above.
310076	Enhance the GTP IMSI/APN table size to 100,000 per VDOM.
356587	Increase SSLVPN Portal tablesize for FG-600C/600D and FG-800C/900D to 128.
305484	Increase LDAP filter string size.
306822	Increase `firewall.address` and `firewall.address6` back to 20000 in FG-600C.

VM

Bug ID	Description
304802	Users may lose access to the HTTPS GUI after upgrading from 5.2.5 due to the `Fortinet_Firmware` certificate being removed FortiView.

Vulnerability

Bug ID	Description
370337	Upgrade OpenSSL to 1.0.2h.

VOIP

Bug ID	Description
363690	SIP ALG changes the *From* field in BYE message causing `error 481` and the call to remain open.

WANopt & Web Proxy

Bug ID	Description
373739	`wad daemon` may stop working when processing HTTPS traffic.
291241	WAD has a `FD` leak after concurrent tests.
271526	A WAD session leak can occur.
309149	Explicit Proxy does not respect assigned outgoing IPs.
304367	SSH protocol handling requires high CPU usage.
364869	`wad` stops responding and experiences high latency when using the `ssl-server` feature.
305488	`wad` to `fnbamd` communication times out.
310931	Explicit proxy does not expand `PROTURI` on the Authentication Login page correctly.
308409	`wad` stops working with signal 11.
305818	Cannot assign custom URL categories inside Explicit Proxy address objects.
305867	Explicit Proxy address group object does not allow *Host Regex* object assignment.
304602	Deep inspection in Proxy Mode can hides weak encryption issues.

WiFi

Bug ID	Description
306612	*Web filter* > *Category* rating is not blocked properly on proxy inspection via HTTP proxy.
363949	The iOS YouTube application is blocked even though the `https certificate-inspection mode` sttings overrides the Web Filter Profile.
188261	EC Registration Protocol and Web Filter override should not share same port number 8010.
305904	Reword the FortiClient error message for mac and Windows to have some info about FortiHeartBeat.
365674	FWF50E/FWF30E hangs when using built-in wireless.
371561	Changed the built-in certificate for WiFi from *Comdo* to *Entrusted*.

Known Issues

The following issues have been identified in version 5.4.1. 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
367514	Executable files may not be blocked by DLP built-in `exe` file-type filter.

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.

FortiGate-98D-POE

Bug ID	Description
372556	FortiGate-98D-POE hardware switch jumbo frame may not work as expected.

FortiGate-3815D

Bug ID	Description
385860	FGT-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.

FortiSwitch

Bug ID	Description
357360	DHCP snooping does not work on IPv6.
374346	Adding or reducing stacking connections may block traffic for 20 seconds.

FortiSwitch-Controller/FortiLink

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

FortiView

Bug ID	Description
289376	Applying the filter *All* by using the right click method may not work in the *All Sessions* page.
303940	*Web Site* > *Security Action* filter may not work.
373142	*Threat: Filter* result may not be correct when adding a filter on a threat and threat type on the first level.
366627	FortiView Cloud Application 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.
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.
374146	Peer certificate may still show up when a editing IPsec VPN tunnel even when setting the `authmethod` pre-shared key.
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.
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.

Bug ID	Description
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.
356985	You may not be able to create *Restrict Google account usage to specific domains* via GUI.
375255	You may not be able to quarantine the FortiClient device in FortiView because of a javascript error.
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
374339	SSL VPN setting page may not check the required fields.
374371	The IPS Predefined Signature information popup window may not be displayed because it is hidden behind the *Add Signature* window.
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.

Bug ID	Description
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.

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.
300637	MUDB logs may display *Unknown* in the Attack Name under UTM logs.
374411	Local and Learning report web usage may only report data for outgoing traffic.

SSL VPN

Bug ID	Description
282914	If users use SSL VPN in Web Mode, they may not be able to access a FortiGate running 5.4.
304528	SSL VPN Web Mode PKI user might immediately log back in even after logging out.
304139	SSL VPN *Login Anyway* might not work when `limit-user-logins` is enabled.
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.

System

Bug ID	Description
304199	FortiLink traffic is lost in HA mode.
304482	NP6 offloading may be lost when the IPsec interface has the `aes256gcm` proposal.
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.

Upgrade

Bug ID	Description
269799	sniffer config may be lost after upgrade.
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.
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.

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