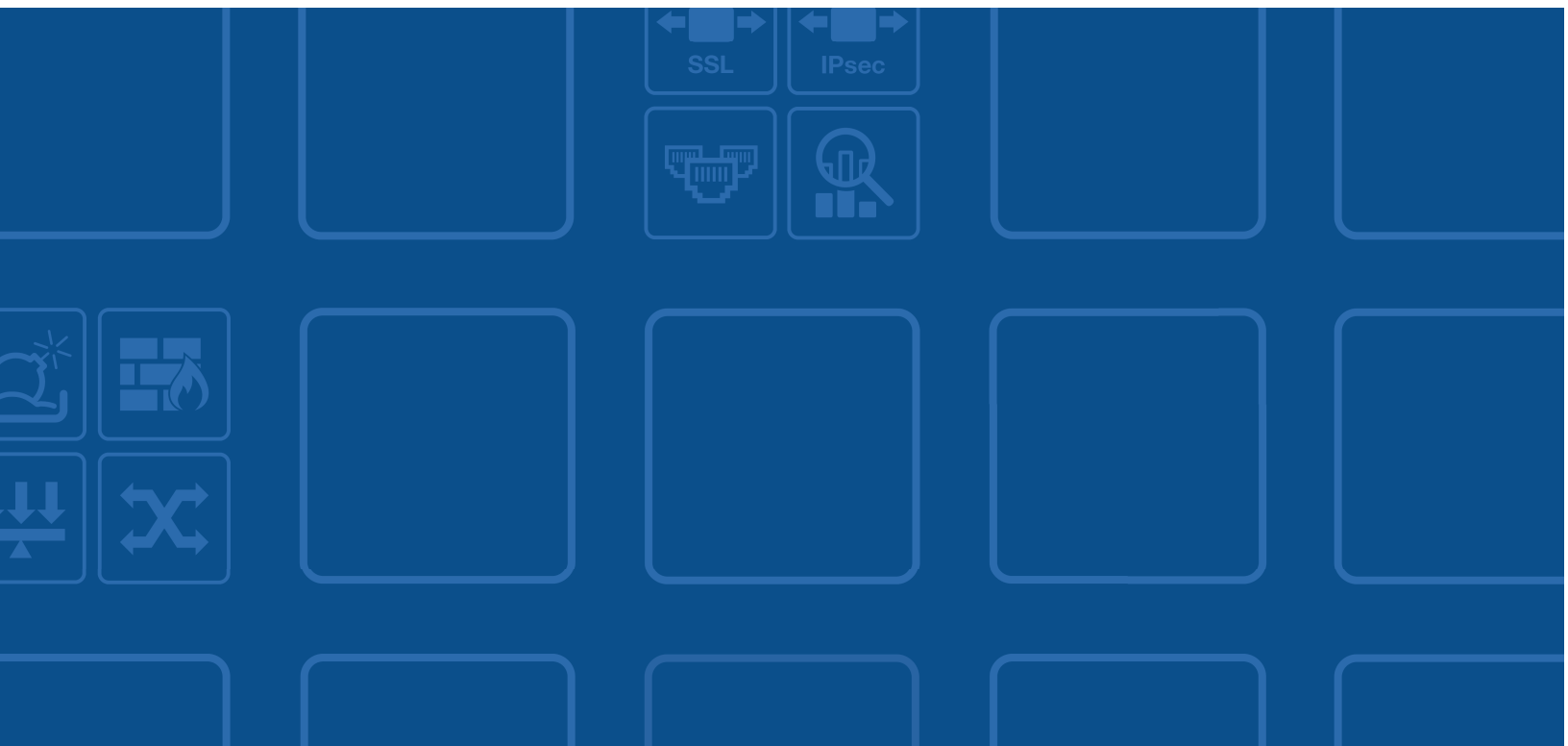
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.4.9



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

https://www.fortinet.com/support-and-training/training.html

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 16, 2019

FortiOS 5.4.9 Release Notes

01-549-488478-20190716

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-05-10	Initial release of FortiOS 5.4.9.
2018-06-01	Updated *Upgrade Information* > *Upgrading to FortiOS 5.6.0 and later*.
2018-06-04	Added 486466 and 416452 to *Known Issues*.
2018-06-08	Added 479311 to *Known Issues*.
2018-06-25	Added 495994 to *Known Issues*.
2018-06-29	Added 403097 to *Known Issues*. Deleted *Special Notices* > *Policy list display changes* > *In Policy & Objects lists*. In *Special Notices*, added section that `config system dedicated-mgmt` is no longer supported.
2019-07-16	Updated 444969 description in *Resolved Issues*.

Introduction

This document provides the following information for FortiOS 5.4.9 build 1202:

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

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.4.9 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-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-3800D, 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-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VMX, FG-VM64-XEN FortiOS 5.4.9 supports the additional CPU cores through a license update on the following VM models: • VMware 16, 32, unlimited • KVM 16 • Hyper-V 16, 32, unlimited
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM
FortiOS Carrier	FortiOS Carrier 5.4.9 images are delivered upon request and are not available on the customer support firmware download page.

Special branch supported models

The following models are released on a special branch of FortiOS 5.4.9. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1202.

FGR-30D	is released on build 7758.
FGR-30D-A	is released on build 7758.
FGR-35D	is released on build 7758.
FG-30E-MI	is released on build 8041.
FG-30E-MN	is released on build 8041.
FWF-30E-MI	is released on build 8041.
FWF-30E-MN	is released on build 8041.
FWF-50E-2R	is released on build 7756.
FG-52E	is released on build 8044.
FG-60E	is released on build 8043.
FG-60E-POE	is released on build 8043.
FG-60E-DSL	is released on build 8040.
FWF-60E	is released on build 8043.
FWF-60E-DSL	is released on build 8040.
FG-61E	is released on build 8043.
FWF-61E	is released on build 8043.
FG-80E	is released on build 8043.
FG-80E-POE	is released on build 8043.
FG-81E	is released on build 8043.
FG-81E-POE	is released on build 8043.
FG-90E	is released on build 8037.
FG-91E	is released on build 8037.

FWF-92D	is released on build 7759.
FG-100E	is released on build 8043.
FG-100EF	is released on build 8043.
FG-101E	is released on build 8043.
FG-140E	is released on build 8043.
FG-140E-POE	is released on build 8043.
FG-200E	is released on build 8038.
FG-201E	is released on build 8038.
FG-300E	is released on build 4220.
FG-301E	is released on build 4220.
FG-500E	is released on build 4220.
FG-501E	is released on build 4220.
FG-2000E	is released on build 8039.
FG-2500E	is released on build 8039.
FG-3960E	is released on build 8036.
FG-3980E	is released on build 8036.
FG-5001E	is released on build 8035.
FG-5001E1	is released on build 8035.
FG-VM64-AZURE	is released on build 8029.
FG-VM64-AZUREONDEMAND	is released on build 8029.
FG-VM64-OPC	is released on build 3479.

What's new in FortiOS 5.4.9

FortiOS 5.4.9 is a bug fix release with no new features.

Special Notices

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate with an RSA 2048-bit key; and FortiOS supports DH group 14 for key-exchange.

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.

Policy list display changes

To improve performance, FortiOS 5.4.6 implemented the following changes when displaying lists in *Policy & Objects*.

In *Policy & Objects* > *Addresses*:

- The *Address* | *Group* | *All* option at the top is removed and all addresses and groups are displayed in sections.
- Paging options at the bottom are removed.
- The group member count is moved to the *Details* column.

In *Policy & Objects* > *Policy* lists:

- The *Sequence* view and *Seq.#* column are removed.
- Custom sections (global-labels) are no longer supported.
- To start searching, press Enter, click the search button, or click outside the search box.
- Column filters are reset when you leave or reload the page.
- Section expand/collapse settings are reset when you leave or reload the page.

FortiAnalyzer support

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

Removed SSL/HTTPS/SMTPS/IMAPS/POP3S

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

FortiGate and FortiWiFi-92D hardware limitation

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

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

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

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

When the command is enabled:

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

When the command is disabled:

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

FG-900D and FG-1000D

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

FG-3700DX

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

FortiGate units managed by FortiManager 5.0 or 5.2

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

FortiClient support

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

Consider the FortiClient license before upgrading. Full featured FortiClient 5.2 and 5.4 licenses will carry over into FortiOS 5.4.1 and later. Depending on your organization's needs, you might need to purchase a FortiClient EMS license for endpoint provisioning. Contact your sales representative 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. You need to purchase a new license for either FortiClient EMS or FortiGate. A license is compatible with 5.4.1 and later if the SKU begins 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 5.4.9, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

FortiClient profile changes

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

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

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

FortiPresence

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

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

Log disk usage

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

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

SSL VPN setting page

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

FG-30E-3G4G and FWF-30E-3G4G MODEM firmware upgrade

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

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

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

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

DLP, AV

In 5.2, Block page was sent to client with HTTP status code `200` by default. In 5.4 and later, Block page is sent to client with a clearer HTTP status code of `403 Forbidden`.

Using ssh-dss algorithm to log in to FortiGate

In version 5.4.5 and later, using `ssh-dss` algorithm to log in to FortiGate via SSH is no longer supported.

config system dedicated-mgmt not supported

The CLI command `config system dedicated-mgmt` is no longer supported. Please use `set dedicated-to`.

Upgrade Information

Upgrading to FortiOS 5.4.9

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

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 a 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.

Upgrading to FortiOS 5.6.0 and later

This only applies if you are upgrading to version 5.6.0 or 5.6.3. If you are upgrading to version 5.6.1, 5.6.2 or 5.6.4, you don't need to reconfigure IPsec settings.

If you have configured IPsec in version 5.4.9 and you upgrade to 5.6.0 or 5.6.3, you must reconfigure all IPsec phase1 `psksecret` settings after upgrading in order to establish an IPsec tunnel.

LDAP server

Starting with FortiOS 5.4.6, `dn` is a mandatory field for LDAP servers. You should set the `dn` field before upgrading to FortiOS 5.4.6 and later to retain the LDAP server configuration. Otherwise, the LDAP server configuration is removed during the upgrade. You can use one of the following methods to prepare for the upgrade:

- Set the `dn` field before upgrading to FortiOS 5.4.6 and later
- Edit the FortiOS backup config to set the `dn` field, and then load the backup config after upgrading to FortiOS 5.4.6 and later

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.

Firewall Policies with Wildcard FQDNs are Deleted

Firewall policies cannot contain wildcard FQDNs. Firewall rules that use wildcard FQDNs are deleted when you upgrade from 5.2.x to 5.4.x. So if you have firewall rules that use wildcard FQDNs, you must reconfigure those rules to remove the wildcards.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.9, 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 5.4.9 support

The following table lists 5.4.9 product integration and support information:

Web Browsers	• Microsoft Edge 38 • Mozilla Firefox version 53 • Google Chrome version 58 • 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 40 • Mozilla Firefox version 53 • Apple Safari version 10 (For Mac OS X) • Google Chrome version 58 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 and later If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading the FortiGate.
FortiClient iOS	• 5.4.1 and later
FortiClient Android and FortiClient VPN Android	• 5.4.0 and later

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

Fortinet Single Sign-On (FSSO)	• 5.0 build 0267 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Server Edition
	  • Windows Server 2016 Datacenter
	  • 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	• 2.6.0 and later. Some FortiGate models may be supported on specific FortiExplorer versions.

FortiExplorer iOS	• 1.0.6 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 3.0.0 • 2.0.2 and later
AV Engine	• 5.247
IPS Engine	• 3.522
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

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

Language support

The following table lists language support information.

Language support

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

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
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2336. Download from the Fortinet Developer Network https://fndn.fortinet.net.

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

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 53 Google Chrome version 58
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 53 Google Chrome version 58
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 53
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 53 Google Chrome version 58
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

SSL VPN host compatibility list

It is recommended to verify the accuracy of the GUID for the software you are using for SSLVPN host check. The following Knowledge Base article at http://kb.fortinet.com/ describes how to identify the GUID for antivirus and firewall products: How to add non listed 3rd Party AntiVirus and Firewall product to the FortiGate SSL VPN Host check.

After verifying GUIDs, you can update GUIDs in FortiOS by using this command:

```
config vpn ssl web host-check-software
```

Following is an example of how to update the GUID for AVG Internet Security 2017 on Windows 7 and Windows 10 by using the FortiOS CLI.

The GUIDs in this example are only for AVG Internet Security 2017 on Windows 7 and Windows 10. The GUIDs might be different for other versions of the software and other operation systems.

To update GUIDs in FortiOS:

1. Use the `config vpn ssl web host-check-software` command to edit the `AVG-Internet-Security-AV` variable to set the following GUID for AVG Internet Security 2017: `4D41356F-32AD-7C42-C820-63775EE4F413`
2. Edit the `AVG-Internet-Security-FW` variable to set the following GUID: `757AB44A-78C2-7D1A-E37F-CA42A037B368`

Resolved Issues

The following issues have been fixed in version 5.4.9. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
386130	MAPI protocol does not exist in SNMP statistics for proxy.
462817	WAD crash with signal 11 (or 6) when sending/receiving emails with attachments through Office 2016.
473976	WAD process crash continuously when AV proxy inspection with third-party explicit proxy traffic is enabled.

Authentication

Bug ID	Description
130461	FortiGate queries RADIUS server too many times when `include in all groups` is enabled in RADIUS server conf.
450443	Remote Authentication Admin User match problem with FortiOS 5.4 and later.
456719	RADIUS attribute `NAS-IP-Address` incorrectly decoded.
457883	Certificate warnings `SAN` missing in Chrome when redirecting to the HTTPS captive portal even though CA cert is trusted.
461373	Explicit proxy kerberos and LDAP group search timeout after upgrade.
464186	`Authd` does not send back full certificate chain to client after certificate is re-signed.

Firewall

Bug ID	Description
398024	SLB SSL offload loading issue with form page.
412967	On FG-200D, packets are not sent to IPS when IPS sensor is only enabled on firewall policy6 in one direction.
441507	Version 5.4.4 and 5.4.5 fails to log denied broadcast traffic in local traffic log.

Bug ID	Description
459615	Session count is incorrect.
462155	Session clash seen for ICMP traffic from the same source IP.
467025	Can't create the second IPv6 VIP64 which has the same ext/int IP with existing one, but different port-forwarding port.
472224	VIP LB health check erroneous status.

GUI

Bug ID	Description
460906	FG-5001D network interface list not showing any interfaces in the GUI.

HA

Bug ID	Description
421335	One time `hasync` crash when running HA scripts for FIPS-CC FGT.
445173	FortiGate scheduled update failed log messages from slave after upgrade to FOS 5.4.5 GA b1138.
450528	HA communication may break when `hasync` restarts.
450928	VLAN HA monitor feature does not work consistently with a large numbers of VLANs.
453884	Filter is not working in case traffic is handled by HA cluster unit without management VDOM (vlcuster).
455513	Management VDOM's I/F address on slave is lost or sync'ed with Master's.
466379	After HA failover, new master unit use an OSPF MD5 authentication encryption sequence that is lower than previous sequence number.
473468	All members of a two-unit cluster becomes a slave role after adding port with status `down` for monitor and the master is rebooted.
474867	FortiGate does not send syslog from `ha-mgmt-interface` after `management-vdom` is changed.
474961	Some daemons should run as master on both units when standalone config sync is enabled.

IPS

Bug ID	Description
460138	When upgrading IPS engine to anything higher than 3.174, Google applications sometimes get blocked.
469608	ICMP packets dropped during FortiGate update.
478319	Applying IPS profile on firewall policy disrupts custom banking application.

IPsec VPN

Bug ID	Description
442671	Setting `broadcast-forward` to enable not working for IPsec interface.
445750	IPsec VPN dialup connection cannot be made when same peer ID configured for tunnels with different WAN links.
465323	After reconnecting IPsec tunnel, IPsec local and remote interface addresses are not installed on SPOKE's routing table.
475751	Encrypted traffic doesn't go through the IPsec tunnel.
476198	IPsec traffic sourced from FW interface not processed correctly by policy.

REST-API

Bug ID	Description
472716	Cannot delete entry in `system.mac-address-table`.

Router

Bug ID	Description
411969	IGMP Membership report with source 0.0.0.0 is discarded by the kernel.
441665	Configured static route is not in IP route list in TP VDOM.
454871	OSPFD process crashes with signal 11 `ospf_external_lsa_refresh`.
459640	OSPF over IPsec tunnel not getting established after VPN restart.
460624	OSVFv3 doesn't inject external route tag field into LSU (LSA 5).
460808	VRRP packets coming from wan1 are not be forwarded to wan2.

Bug ID	Description
463576	Parameter to `rtnl_open` needs to be changed to prevent possible problems.
468451	Multicast flow takes 10 seconds to be forwarded if the receiver joins the group first.
476710	Policy route members table is not getting updated on WAN LLB setup.

Spam

Bug ID	Description
416790	"(no.x pattern matched)" is not logged when BWL matches envelope MAIL FROM.
466606	Emails tagged as SPAM - Whitelist is not effective.
479703	Issue with `Spamfilter - Local` override and order of execution.

SSL VPN

Bug ID	Description
391314	SSL VPN connections are disconnected if you delete any CA.
405334	Soc3 platform SSL VPN cannot be accessed after `set sslvpn-kxp-hardware-acceleration disable`.
407604	FG-92D SSL VPN daemons restart after a new VDOM is created.
440853	RDP over web-mode SSL VPN to a Windows Server changes the time zone to GMT.
441854	Disabling `skip-check-for-unsupported-os` blocks SSL VPN web access.
458686	RDP fails in SSL VPN if policy with FQDN object is on top.
460145	SSL VPN user not prompted for a token.

Switch

Bug ID	Description
476850	Connection failure issue after moving PC between software switch ports via L2switch.

System

Bug ID	Description
444969	If disk logging is enabled, memory usage of the `reportd` process increases.
450685	Possible corruption in CMDB.
451639	When SSL-SSH-Profile is set to *Protect SSL Server* and `webcache-https` is enabled, FortiGate negotiates with its unit's certificate.
452470	`SYN_SENT` counts differ between `diag sys session full-stat` and `diag sys session list` when setting filter `proto-state` to `2`.
456439	No system log generated for successful admin login with read-only privilege.
460385	Kernel panic on FG-201E v5.4.6.
462000	`ssl.root` interface disappears from slave blade of SLBC cluster.
462457	Kernel routes learnt from old ELBC master never expire on worker blade that are never master.
462875	Hostapd crash with `*** signal 11 (Segmentation fault) received ***`.
466435	Cross NP traffic on a VLAN interface configured over Aggregate interface is not forwarded.
467060	Virtual WirePair wrongly tag the VLAN when passing from Native VLAN to Tagged VLAN.
467887	Replace ARIA and SEED lib file in FOS.
468090	FWF-90D gets kernel panic and hangs.
468124	VDOM license 50 not allowing to create new 11th VDOM.
470399	FG-500E reboots with kernel panic errors.
470408	Cannot create new VDOM even though a license extension has been added to both cluster units.
471110	Intermittently seeing *interface unloaded* messages for all VDOMs in transparent mode.
476302	Traffic blocked on FG-300E/500E when NP6 offloading is enabled.
488861	Kernel panic and reboot.

Upgrade

Bug ID	Description
406973	(Post-upgrade issue from 5.2) Unable to use partial matching of `OU` in `user.peer`.
462209	Checksum mismatch on master and backup FGT-VM64 (VM00) over ESXi 6.0.

VM

Bug ID	Description
379015	Forticron signal 11 crash after changing VCPU allocation to over 82 cores.
468671	FGT1K5D kernel panic after upgrading.

Web Filter

Bug ID	Description
476042	A rare case potentially causes ftgd rating error.

WebProxy

Bug ID	Description
404918	WAD crash.
423480	WAD process crashing with signal 11.
439808	WAD consumes memory until conserve mode.
442894	WAD memory leak.
444257	SSL Deep Inspection breaks for many SSL sites using Chrome.
453933	WAD daemon crashed.
461943	WAD high memory.
471955	WAD memory corruption affects web access.
476708	Internal WAD user counter gets stuck.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
438599	FortiOS 5.4.9 is no longer vulnerable to the following CVE Reference: • CVE-2005-4900
452384	FortiOS 5.4.9 is no longer vulnerable to the following CVE Reference: • CVE-2017-14185
453971	FortiOS 5.4.9 is no longer vulnerable to the following CVE Reference: • CVE-2017-14187
454452	FortiOS 5.4.9 is no longer vulnerable to the following CVE Reference: • CVE-2016-2183

Known Issues

The following issues have been identified in version 5.4.9. 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).

Endpoint Control

Bug ID	Description
374855	Third party compliance may not be reported if FortiClient has no AV feature.
375149	FortiGate does not auto update AV signature version while Endpoint Control (`fortiheartbeat`) is enabled but no AV profile is used.

Firewall

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

FortiGate-3815D

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

FortiRugged-60D

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

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.

Bug ID	Description
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch authorizes successfully but fails to pass traffic until you reboot FortiSwitch.

FortiView

Bug ID	Description
368644	*Physical Topology: Physical Connection* of stacked FortiSwitch may be incorrect.
372350	*Threat view: Threat Type and Event* information is missing in the last level of the threat view.
375187	Using realtime auto update may increase chrome browser memory usage.

GUI

Bug ID	Description
289297	Threat map may not be fully displayed when screen resolution is not big enough.
297832	Administrator with read-write permission for *Firewall Configuration* is not able to read or write firewall policies.
355388	The *Select* window for remote server in remote user group may not work as expected.
365223	In Security Fabric topology, a downstream FortiGate may be shown twice when it uses hardware switch to connect upstream.
365317	Unable to add new AD group in second FSSO local polling agent.
365378	You may not be able to assign `ha-mgmt-interface` IP address in the same subnet as another port from the GUI.
368069	Cannot select `wan-load-balance` or members for incoming interface of IPsec tunnel.
369155	There is no `Archived Data` tab for email attachment in the DLP log detail page.
372908	The interface tooltip keeps loading the VLAN interface when its physical interface is in another VDOM.
373363	Multicast policy interface may list the `wan-load-balance interface`.
373546	Only 50 security logs may be displayed in the *Log Details* pane when more than 50 are triggered.

Bug ID	Description
374081	`wan-load-balance interface` may be shown in the address associated interface list.
374162	GUI may show the modem status as `Active` in the `Monitor` page after setting the modem to disable.
374224	The *Ominiselect* widget and *Tooltip* keep loading when clicking a newly created object in the *Firewall Policy* page.
374320	Editing a user from the *Policy* list page may redirect to an empty user edit page.
374322	*Interfaces* page may display the wrong MAC Address for the hardware switch.
374363	Selecting *Connect to CLI* from managed FAP context menu may not connect to FortiAP.
374373	*Policy View: Filter* bar may display the IPv4 policy name for the IPv6 policy.
374397	Should only list `any` as destination interface when creating an explicit proxy in the TP VDOM.
374521	Unable to *Revert* revisions in GUI.
374525	When activating the *FortiCloud/Register-FortiGate*, clicking *OK* may not work the first time.
375036	The *Archived Data* in the *Sniffer Traffic* log may not display detailed content and download.
375227	You may be able to open the dropdown box and add new profiles even though errors occur when editing a *Firewall Policy* page.
375259	`Addrgrp` editing page receives a `js` error if `addrgrp` contains another group object.
375346	You may not be able to download the application control packet capture from the forward traffic log.
375369	May not be able to change IPsec `manualkey config` in GUI.
375383	The *Policy* list page may receive a `js` error when clicking the search box if the policy includes `wan-load-balance interface`.
379050	User Definition intermittently not showing assigned token.

HA

Bug ID	Description
403097	Some IPsec SAs not synced to HA slave.
479311	Certificate status changes from *OK* to *Pending* one minute after importing certificate from GUI on vcluster device.

IPsec

Bug ID	Description
393958	Shellshock attack succeeds when FGT is configured with `server-cert-mode replace` and an attacker uses `rsa_3des_sha`.
435124	Cannot establish IPsec phase1 tunnel after upgrading from version 5.4.5 to 5.6.0. Workaround: After upgrading to 5.6.0, reconfigure all IPsec phase1 `psksecret` settings.
439923	IKE static tunnels using `set peertype one` may fail to negotiate.

Router

Bug ID	Description
299490	During and after failover, some multicast groups take up to 480 seconds to recover.

SSL VPN

Bug ID	Description
303661	The Start Tunnel feature may have been removed.
304528	SSL VPN Web Mode PKI user might immediately log back in even after logging out.
374644	SSL VPN tunnel mode Fortinet bar may not be displayed.
382223	SMB/CIFS bookmark in SSL VPN portal doesn't work with DFS Microsoft file server error "Invalid HTTP request".

System

Bug ID	Description
287612	Span function of software switch may not work on FortiGate-51E/FortiGate-30E.
290708	`nturbo` may not support CAPWAP traffic.
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
304199	FortiLink traffic is lost in HA mode.
371320	`show system interface` may not show the *Port* list in sequential order.
372717	Option `admin-https-banned-cipher` in `sys global` may not work as expected.

Bug ID	Description
392960	FOS support for V4 BIOS.
416452	Admin profiles with addresses read-write permission will not work for reputation/VIP/address page.
445383	Traffic cannot go through LACP static mode interface with NP6 offload enabled.
486466	HTTPS web page is blocked after clicking *Proceed* button.

Upgrade

Bug ID	Description
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.
495994	After upgrading to 5.4.9, observing a lot of IPS syntax errors on the console screen.

Visibility

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

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.

Traffic shaping limitation for NP6 interfaces

NP6 interfaces on FortiGate devices don't fully support bandwidth limits. When you set the outbandwidth setting on an NP6 interface, the FortiGate implements a lower bandwidth limit than the one that you configure. The inbandwidth setting has no effect on an NP6 interface, unless you disable NP offloading for the traffic on that interface.

FORTINET®

High Performance Network Security