FortiOS - Release Notes

VERSION 5.6.0

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

January 09, 2018

FortiOS 5.6.0 Release Notes

01-560-387824-20180109

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-03-30	Initial release.
2017-03-31	Added FWF-60D to *Introduction* > *Supported models*. Added 401511 to *Resolved Issues*. Removed 402714 from *Known Issues*.
2017-04-03	Added 374501 to *Resolved Issues*.
2017-04-06	Added FG-80D to *Supported models*. Added 378870 to *Resolved Issues*.
2017-04-07	Added 415380 to *Known Issues*.
2017-04-10	Added *Special Notices* > *Use of dedicated management interfaces (mgmt1 and mgmt2)*.
2017-04-12	Added 376808/378744 to *Resolved Issues*. Updated *Product Integration and Support* > *SSL VPN support*.
2017-04-19	Added Windows Server 2016 Standard to *Product Integration and Support* > *FortiOS 5.6.0 support* > *Fortinet Single Sign-On (FSSO)*.
2017-04-21	Added 405122 to *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2017-04-25	Added *Special Notices* > *FortiGate and FortiWiFi-92D Hardware Limitation*. Added FG-60D-POE and FWF-60D-POE to *Supported models*.
2017-05-05	Added warning not to use port 4433 in *Upgrade Information* > *Upgrading to FortiOS 5.6.0*. Added 412184 to *Known Issues*.
2017-05-10	Added 416673 to *Known Issues*.
2017-05-12	In *Upgrade Information*, added link to Supported Upgrade Paths page for upgrading from older versions.
2017-05-15	Added 412293 to *Resolved Issues*.

Date	Change Description
2017-05-24	Added 396236 to *Resolved Issues*.
2017-06-08	SSL VPN standalone client no longer supports Windows operating systems. If you have configured IPsec in FortiOS 5.4.5 or higher, do not upgrade to version 5.6.0. Added 435124 to *Known Issues*.
2017-06-13	Updated *Upgrade Information > Upgrading to FortiOS 5.6.0*. Updated 435124 in *Known Issues*.
2017-08-08	Added 408239 to *Resolved Issues*.
2017-11-03	Added 375170 to *Resolved Issues*.
2017-11-10	Added 273973 to *Known Issues*.
2017-11-30	Added 399871 to *Resolved Issues*.
2018-01-09	Added 454259 to *Known Issues*. Moved 364280 to *Special Notices > Using ssh-dss algorithm to log in to FortiGate*.

Introduction

This document provides the following information for FortiOS 5.6.0 build 1449:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.6.0 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, 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-3800D, FG-3810D, FG-3815D, FG-5001C, FG-5001D
FortiWiFi	FWF-30D, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, 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 5.6.0 images are delivered upon request and are not available on the customer support firmware download page.

What's new in FortiOS 5.6.0

For a list of new features and enhancements that have been made in FortiOS 5.6.0, see the *What's New for FortiOS 5.6.0* document.

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.

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.

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 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.0, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

FortiClient Profile Changes

With introduction of the Security Fabric, 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.

The FortiClient profile on FortiGate is for FortiClient features related to compliance, such as Antivirus, Web Filter, Vulnerability Scan, and Application Firewall. You may set the *Non-Compliance Action* setting to *Block* or *Warn*. FortiClient users can change their features locally to meet the FortiGate compliance criteria. You can also use FortiClient EMS to centrally provision endpoints. The EMS also includes support for additional features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

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.

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.

Upgrade Information

Upgrading to FortiOS 5.6.0

FortiOS version 5.6.0 officially supports upgrading from version 5.4.3 and 5.4.4. To upgrade from other versions, see Supported Upgrade Paths.

If you have configured IPsec in version 5.4.5, after upgrading to 5.6.0, you must reconfigure all IPsec phase1 `psksecret` settings before you can establish an IPsec tunnel.

Before upgrading, ensure that port 4433 is not used for `admin-port` or `admin-sport` (in `config system global`), or for SSL VPN (in `config vpn ssl settings`).

If you are using port 4433, you must change `admin-port`, `admin-sport`, or the SSL VPN port to another port number before upgrading.

Security Fabric Upgrade

FortiOS 5.6.0 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 5.6.0
- FortiClient 5.6.0
- FortiClient EMS 1.2.0
- FortiAP 5.4.2 and later
- FortiSwitch 3.5.2 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

Before upgrading any product, you must read the *FortiOS Security Fabric Upgrade Guide*.

FortiClient Profiles

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

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

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

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

With FortiOS 5.6.0, endpoints in the Security Fabric require FortiClient 5.6.0. You can use FortiClient 5.4.3 for VPN (IPsec VPN, or SSL VPN) connections to FortiOS 5.6.0, but not for Security Fabric functions.

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

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.0, FortiGate-VM v5.6 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.

If you have long VDOM names, you must shorten the long VDOM names (maximum 11 characters) before downgrading:

1. Back up your configuration.
2. In the backup configuration, replace all long VDOM names with its corresponding short VDOM name. For example, replace `edit <long_vdom_name>/<short_name>` with `edit <short_name>/<short_name>`.
3. Restore the configuration.
4. Perform the downgrade.

Amazon AWS Enhanced Networking Compatibility Issue

With this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.6.0 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 5.6.0 to older versions, 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 5.6.0 support

The following table lists 5.6.0 product integration and support information:

Web Browsers	• Microsoft Edge 25 • Microsoft Internet Explorer version 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 version 11 • Mozilla Firefox version 45 • Google Chrome version 51 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Security Fabric Upgrade on page 11. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Security Fabric Upgrade on page 11. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	See important compatibility information in Security Fabric Upgrade on page 11. • 5.6.0 If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.

FortiClient iOS	• 5.4.3 and later
FortiClient Android and FortiClient VPN Android	• 5.4.0
FortiAP	• 5.4.2 and later • 5.6.0
FortiAP-S	• 5.4.3 and later • 5.6.0
FortiSwitch OS (FortiLink support)	• 3.5.2 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.0 and later

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

FortiExtender	• 3.1.1
AV Engine	• 5.239
IPS Engine	• 3.410
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, 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 v5.6 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
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2333. 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 52 Google Chrome version 56
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 52 Google Chrome version 56
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 52

Operating System	Web Browser
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 52 Google Chrome version 56
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

SSL VPN host compatibility list

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

Supported Microsoft Windows XP antivirus and firewall software

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

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔

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

Firewall

Bug ID	Description
398673	For the `NGFW_vdom`, `App_category`, and `URL_category` in NGFW, `action=pass` firewall policy doesn't work as expected.

FortiRugged 60D

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

FortiGate 80D

Bug ID	Description
373127	FG-80D VLAN interface does not receive packets.

FortiGate 92D

Bug ID	Description
267347	FG-92D does not support hardware switch.

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 is enabled.
402054	Non-registered endpoint user is missing *I understand* button on the warning portal.

FortiView

Bug ID	Description
372350	Threat view: Threat Type and Event information are missing at the lowest level.
373142	The filter result of Threat View may not be correct when adding a filter on a threat and threat type on the first level.
374947	FortiView may show empty country in the IPv6 traffic because country info is missing in log.

GUI

Bug ID	Description
355388	The *Select* window for remote server in remote user group may not work as expected.
365223	CSF: downstream FortiGate may be shown twice when it uses hardware switch to connect upstream.
365378	You may not be able to assign `ha-mgmt-interface` IP address in the same subnet as another port from the GUI.
372943	Explicit proxy policy may show a blank for default authentication method.
373127	FG-80D VLAN interfaces may fail to pass traffic.
374146	Peer certificate may still show up when editing IPsec VPN tunnel and even when setting the authmethod pre-shared key.
374166	Using Edge cannot select the firewall address when configuring a static route.
374221	SSL VPN setting portal mapping realm field misses the / option.
374237	You may not be able to set a custom NTP server using GUI if you did not config it using CLI first.
374322	*Interfaces* page may display the wrong MAC Address for the hardware switch.
374343	After enabling `inspect-all` in `ssl-ssh-profile`, user may not be able to modify `allow-invalidserver-cert` from GUI.
374363	Selecting Connect to CLI from managed FAP context menu may not connect to FortiAP.
374371	The IPS Predefined Signature information pop up window may not be seen as it is hidden behind the Add Signature window.
374521	Unable to Revert revisions on GUI.

Bug ID	Description
375255	You may not be able to quarantine the FortiClient device in FortiView because of a javascript error.
375259	Addrgrp editing page receives a js error if addrgrp contains another group object.
375290	Fortinet Bar may not be displayed properly.
375346	You may not be able to download the application control packet capture from the forward traffic log.
376808, 378744	The proxy.pac file is not updated according to changes from GUI.
403655	GUI has issue loading some web pages with IE 11 and Edge web browsers.
404781	Setup wizard does not work properly.
407030	Interface bandwidth widget is always loading for newly added interfaces.
407060	Some right-click menu items are missing icon on policy and firewall object list page.
407284	FortiView encounters JavaScript in non-root VDOM and FortiView from FortiAnalyzer.
408908	GUI has issue creating a site2site IPsec tunnel with authmethod psk.
409594	Unable to create VLAN interface for non-management VDOM at 'Global' view.

HA

Bug ID	Description
375170	HA fldb sync log message shows strange version number.
409707	User cannot login to FGT after restore config in HA.
412293	HA GARP (Gratuitous ARP) should be sent immediately after failover.

IPsec

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

Kernel

Bug ID	Description
395515	ICMP unreachable message processing causes high CPU usage in kernel and DHCP daemon.

Log & Report

Bug ID	Description
300637	MUDB logs may display Unknown in the Attack Name field under UTM logs.
367247	FortiSwitch log may not show the details in GUI, while in CLI the details are displayed.
374103	Botnet detection events are not listed in the Learning Report.
374411	Local and Learning report web usage may only report data for outgoing traffic.
399871	Inconsistent log fields values - some have double quotes and other don’t.
401511	FortiGate local report shows incorrect malware victims and malware sources.

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.
375137	SSL VPN bookmarks may be accessible after accessing more than ten bookmarks in web mode.
396236	Support SSL VPN as source interface for WAN LLB.
408281	IE 11 and Safari browsers cannot load SSL VPN web portal page.
409755	iOS FortiClient 5.4.3.139 fails to connect to SSL VPN tunnel mode.

System

Bug ID	Description
287612	Span function of software switch may not work on FortiGate 51E or FortiGate 30E.
304482	NP6 offloading may be lost when the IPsec interface has the aes256gcm proposal.
371320	Show system interface may not show the Port list in sequential order.
371986	NP6 may have issue handling fragment packets.

Bug ID	Description
372717	Admin-https-banned-cipher in sys global may not work as expected.
378870	When AV mode is flow-mode, the counters of `fgAvStatsEntry` cannot be counted up.
402589	Cannot forward traffic in TP VDOM with NP6Lite NPU VDOM link.
409198	System time zone may not take effect.
409203	Firewall recurring schedule does not work with time range.

Visibility

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

WiFi

Bug ID	Description
409670	mpsk-key entries do not allow saving passphrase in encrypted format.

Common Vulnerabilities and Exposures

Bug ID	Description
374501	FortiOS 5.6.0 is no longer vulnerable to the following CVE Reference: • 2016-0723 Visit https://fortiguard.com/psirt for more information.
378697	FortiOS 5.6.0 is no longer vulnerable to the following CVE Reference: • 2016-2512 Visit https://fortiguard.com/psirt for more information.
379870	FortiOS 5.6.0 is no longer vulnerable to the following CVE Reference: • 2003-1418 • 2007-6750 Visit https://fortiguard.com/psirt for more information.
383538	FortiOS 5.6.0 is no longer vulnerable to the following CVE Reference: • 2016-3713 • 2016-5829 Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
383564	FortiOS 5.6.0 is no longer vulnerable to the following CVE Reference: • 2016-5696 Visit https://fortiguard.com/psirt for more information.
405122	FortiOS5.6.0 is no longer vulnerable to the following CVE Reference: • 2016-7055 • 2017-3732 Visit https://fortiguard.com/psirt for more information.
408239	FortiOS5.6.0 is no longer vulnerable to the following CVE Reference: • 2015-8874 • 2016-5766 • 2016-5767 • 2016-6128 • 2016-6132 • 2016-6207 • 2016-6912 • 2016-9317 • 2016-10166 • 2016-10167 • 2016-10168 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.6.0. 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).

Firewall

Bug ID	Description
412799	`auto-asic-offload` disable does not work for `NGFW` policy.

FortiGate 800D

Bug ID	Description
404228	All the interfaces status are down except mgmt after cfg revert.

FortiGate 3815D

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

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch authorizes successfully, but fails to pass traffic until you reboot FortiSwitch.
404399	FortiLink goes down when connecting to ForiSwitch 3.4.2 b192.
408082	Operating a dedicated hardware switch into FortiLink changes STP from *enable* to *disable*.
415380	DHCP snooping enabled on FortiSwitch VLAN interfaces may prevent clients from obtaining addresses through DHCP. The workaround is to disable `switch-controller-dhcp-snooping` on FortiLink VLAN interfaces.

FortiView

Bug ID	Description
366627	FortiView Cloud Application may display the incorrect drill down *File and Session* list in the *Applications View*.
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.

GUI

Bug ID	Description
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.
373546	Only 50 security logs may be displayed in the Log Details pane when more than 50 are triggered.
374247	GUI list may list another VDOM interface when editing a redundant interface.
374373	*Policy View: Filter* bar may display the IPv4 policy name for the IPv6 policy.
375036	The *Archived Data* in the *Sniffer Traffic* log may not display detailed content and download.
397010	GUI does not display the `App-DB` and `INDUSTRIAL-DB` information.
413754	GUI create VDOM link on TP VDOM fails with error.
413891	In *Topology* > *FortiAnalyzer*, clicking *Configure setting* redirects to VDOM security fabric page.
413921	In FSSO standard mode, context menu allows you to delete ad-groups polled from CA.
454259	The *Policy* list page does not display tooltips for policy comments.

HA

Bug ID	Description
414336	Slave cannot sync to master with redundant interface.
416673	The *System* > *HA* pane is not in the GUI. HA is supported and can be configured in the CLI.

IPsec

Bug ID	Description
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.

Log & Report

Bug ID	Description
396319	For the NGFW_vdom, the application UTM log action is always PASS when firewall policy deny the traffic.
412649	In NGFW Policy mode, FGT does not create webfilter logs.
413778	With long VDOM names, no log is displayed when only one field subtype forward is added to traffic log filter.

Security Fabric

Bug ID	Description
385341	If there are multiple FortiAPs managed, GUI cannot display managed FortiAPs in *FortiView > Physical Topology* page.
403085	The session tab cannot be displayed on historical page when you drill down into the members.
403229	FortiGate is unable to drill down to the final level when using FortiAnalyzer as logging device.
406561	Matching username is not highlighted in tooltip after topology search.
408495	An improper warning message may appear in the FortiAnalyzer log when changing the root FortiGate to a downstream FortiGate.
409156	An unlicensed FortiGate may be marked as *Passed* in Firmware & Subscriptions.
411368	Multiple MAC addresses may be displayed abnormally in `Device` field.
411479	The icon used to signify the souce of logs when the time range is set to now is incorrect.
411645	Drilling down to an upstream FortiGate from a downstream FortiGate may produce a blank page.
412104	The drill down for an aggregated device is not displayed as an individual device.
412249	Threats of a downstream FortiGate cannot be displayed on the root FortiGate.

Bug ID	Description
412930	Security Audit Event are shown incorrectly in the security fabric child nodes.
413189	The bubble chart with FortiAnalyzer view may not be drawn correctly.
413492	CSF topology change can cause high CPU usage by `miglogd` on CSF root.
413742	A red circle to indicate the root node of the security fabric may be displayed on each child FortiGate.
413912	An upstream FortiGate may still be displayed incorrectly when Security Fabric is disabled on a downstream FortiGate.
414013	The FortiGate may produce an “Internal CLI error” on GUI when changing the logging mode from default to local.
414147	The topology fails to be updated after changing the upstream port on a child FortiGate.
414301	Security Fabric topology will not be displayed due to js error if managed FortiSwitches have redundant topology.

SSL VPN

Bug ID	Description
304528	SSL VPN Web Mode PKI user might immediately log back in even after logging out.
396788	SSL VPN GUI is unable to keep SSO password information for user bookmark.
413758	Auto-generated SSL interface do not 't associate with `SSLVPN_TUNNEL_ADDR1` for a long name VDOM.

System

Bug ID	Description
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.
410916	FG-5001D might encounter kernel panic after set split port.
412184	Do not use port 4433 for the `admin-port`, `admin-sport`, or the SSL VPN port; otherwise you cannot access FortiGate.

Bug ID	Description
412244	Fortitoken Mobile push won't work when VDOM is enabled.
413885	`long-vdom-name` is disabled after `exe factoryrest2`.
414482	`miglogd` might keep crashing if more than 50000 polices are configured.
414490	FG-101E might hang after reboot.

Upgrade

Bug ID	Description
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.

WiFi

Bug ID	Description
382296	Unable to redirect HTTPS FortiGuard web filtering block page when deploying webfilter with deep inspection on IE and Firefox.
413693	WPA_Entreprise with Radius Auth mode fails with VDOM that has a long VDOM name.

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.