FortiOS - Release Notes

VERSION 5.6.1

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

FORTINET®

June 18, 2018

FortiOS 5.6.1 Release Notes

01-561-442374-20180618

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-07-27	Initial release.
2017-07-28	Added 436437 to *Resolved Issues*.
2017-07-31	Added 392677 to *Resolved Issues*.
2017-08-02	In *Resolved Issues*, added 415416 and updated 440744.
2017-08-04	Added 442808 to *Known Issues*.
2017-08-16	Added 445373 to *Known Issues*.
2017-09-05	Added 408321 to *Resolved Issues*.
2017-11-10	Added 273973 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*.
2018-02-15	Added 422382 to *Resolved Issues*.
2018-02-23	Added 441837 / 441854 to *Resolved Issues*.
2018-04-27	Added 369437 to *Resolved Issues*.
2018-05-17	Added CVE number to 438599 in *Resolved Issues*.
2018-06-18	Deleted 374247, 375036, and 439185 from *Known Issues*.

Introduction

This document provides the following information for FortiOS 5.6.1 build 1484:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.6.1 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-140E, FG-140E-POE, FG- 200D, FG-200D-POE, FG-200E, FG-201E, 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-2000E, FG-2500E, 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 5.6.1 images are delivered upon request and are not available on the customer support firmware download page.

What’s new in FortiOS 5.6.1

For a list of new features and enhancements that have been made in FortiOS 5.6.1, see the *What’s New for FortiOS 5.6.1* 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 5.6.1, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

FortiClient Profile Changes

With introduction of the Fortinet 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 5.6.1

FortiOS version 5.6.1 officially supports upgrading from version 5.4.4, 5.4.5, and 5.6.0. To upgrade from other versions, see Supported Upgrade Paths.

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

- FortiAnalyzer 5.6.0
- FortiClient 5.6.0
- FortiClient EMS 1.2.1
- 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 5.6.1, 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 5.6.1, 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 5.6.1 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 5.6.1 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 5.6.1 support

The following table lists 5.6.1 product integration and support information:

Web Browsers	• Microsoft Edge 38 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 54 • Google Chrome version 59 • 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 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 53 • Google Chrome version 58 • Apple Safari version 10 (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 10. 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 10. 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 10. • 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	• 5.4.1 and later
FortiAP	• 5.4.2 and later • 5.6.0
FortiAP-S	• 5.4.3 and later • 5.6.0
FortiSwitch OS (FortiLink support)	• 3.5.6 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 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 Datacenter • 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 FSSO does not currently support IPv6.
FortiExtender	• 3.1.1 and later
AV Engine	• 5.247
IPS Engine	• 3.426
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	✔

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 54 Google Chrome version 59
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54

Operating System	Web Browser
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 54 Google Chrome version 59
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 5.6.1. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
374969	FortiSandbox FortiView may not correctly parse the FSA v2.21 tracer file (.json).
398332	FortiSandbox results are not showing up in FortiView > FortiSandbox.
408147	Virus detected with correct name but wrong `virusid`.
411432	`scanunitd` causes high CPU usage when making configuration changes.

Authentication

Bug ID	Description
402621	Radius *Accounting Packet Calling-Station-ID* field should return MAC address instead of IP address.
403147	Cannot create guest users with short phone number.
412846	Google Chrome browser display `NET::ERR_CERT_COMMON_NAME_INVALID` certificate waning on authentication page.
416618	LDAP does not work when number of matching entries is even in user group.
437204	`authd` sends malformed NTLM TYPE2 to browser and breaks NTLM authentication.
438972	Nested Groups in LDAP authentication does not work when the *Domain users* in AD is not the Primary Group.

DLP

Bug ID	Description
367514	Executable files may not be blocked by DLP built-in .exe file-type filter.
416469	DLP quarantined IP when the action is set to block/log-only.
422355	DLP file-type filter cannot detect .mov file during file upload.

DNSFilter

Bug ID	Description
414243	DNSFilter local FortiGuard SDNS servers failed to respond due to malformed packet.
422407	`dnsproxy` causes high CPU usage and degradation of DNS traffic.

FOC

Bug ID	Description
406692	GTP `noip-filter` blocking IPv6 gtp-u traffic.
412883	Over-subscription of TP2 XAUI when running GTP in LAG with FG3700DX platform.

FortiGate 92D

Bug ID	Description
412432	`fgt92d_link` running in `D` state.

FortiLink

Bug ID	Description
422750	FortiGate sending corrupted configuration to FortiSwitch.
435219	`cu_acd` causing memory leak leading to Conserve Mode.
438973	Managed FortiSwitch speed setting not synced in FortiGate HA cluster.

FortiView

Bug ID	Description
378576	The All Sessions > filter application on historical view does not work and suggests adding filter for destination port.
390495	Unable to view web sites in FortiView for 5 minutes, 1 hour, and 24 hours.

Firewall

Bug ID	Description
305575	In the Policy List, the NAT column can give more useful information.
416111	FQDN address is unresolved in a VDOM, although the URL is resolved with IP.

Bug ID	Description
416678	FG-100E and FG-101E may have firewall lockups in production.
424558	Renaming onetime schedule causes policy activation.
433688	Netflow report for a long, live FTP session is incorrect.
435070	Full Cone NAT not working for WhatsApp video and voice call.
435095	FortiOS ICMP replies or error messages are dropped when asymmetric routing is involved.
435700	RSTP session-helper does not modify the IP in describe payload when the server IP is a VIP.

GUI

Bug ID	Description
310497	Improve GUI error message when trying to create a VLAN interface and physical interface is not selected.
368069	Cannot select `wan-load-balance` or members for incoming interface of IPsec tunnel.
373546	Only 50 security logs may be displayed in the Log Details pane when more than 50 are triggered.
373602	Cannot access *System* > *Advanced* from the GUI - page keep loading.
374373	*Policy View: Filter* bar may display the IPv4 policy name for the IPv6 policy.
380943	Webfilter profile, GUI to support search in URL filter table.
388104	Interface list *expand* column display improperly in VLAN interface in a Zone.
394359	REST API firewall policy lookup does not work properly.
397010	GUI does not display the `App-DB` and `INDUSTRIAL-DB` information.
398394	Log viewer, negative filter for severity Information field cannot be done manually.
407938	`device-access-list` configuration is removed when making a change to the interface in the GUI.
408577	Admin and FortiClient profile cannot be displayed when language is Japanese.
413754	GUI create VDOM link on TP VDOM fails with error.
413891	In *Topology* > *FortiAnalyzer*, clicking *Configure setting* redirects to VDOM security fabric page.

Bug ID	Description
413921	In FSSO standard mode, context menu allows you to delete ad-groups polled from CA.
415326	CLI configuration for address object allows IP range 0.0.0.0-x.x.x.x, but not in GUI.
418534	IP address, DHCP, allowaccess disappeared when selecting a local-bridge SSID as a member in soft-switch interface.
421263	Multiple wildcard login accounts gives wrong guest account provisioning when `Post-login-banner` is enabled.
423410	Zone interface shows as down in the IPv4 Policy page even when its member is up.
434613	GUI cannot select HA monitor interfaces in other VDOMs.
438709	GUI system time is incorrect when setting timezone.
438948	*Address object length name* is limited in CLI Console tool.
441350	Trying to access the root FortiGate Security Fabric dashboard produces `Error 404`.

HA

Bug ID	Description
369437	HA Sync status icon is missing for Slave's GUI.
392677	The HA widget shows the slave status as *Not Synchronized* even when the status is synchronized.
404089	Uninterruptible upgrade fails because routes are not yet synced with new master.
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.
421639	HA kernel routes are not flushed after failover when cluster has a large number of routes.
423144	Reliable syslog using dedicated HA management interface doesn’t work.
434800	SNMP trap does not reach SNMP server via HA Master when hbdev interface is up.
437390	HA failover triggered before `pingserver-failover-threshold` is reached.
438374	HA reserved management interface unable to access or ping.

IPS

Bug ID	Description
412470	When a firewall policy is deleted, traffic is lost.
417411	One-ARM sniffer logs sent/revd shown in reverse direction.
434478	Information incorrect in `diag test app ipsmonitor 13`.
434592	`Ethernet.IP` is not recognized in `ICS app ctrl` signature by sniffer mode.

IPsec

Bug ID	Description
401847	Half of IPsec tunnels traffic lost 26 minutes after powering on a spare FG-1500D.
408321	If phase2 proposal is configured as `NULL-MD5` encryption, the remote gateway in `diag vpn tunnel list` is changed after receiving traffic from IPsec tunnel.
412863	NP6 drops fragment packet with payload 15319 bytes or higher.
412987	IPsec VPN certificate not validated against PKI user's CN and Subject.
414899	Apple Cisco IPsec VPN group name (IKE ID) length limit.
415353	Telnet connection timing out with IPsec through MPLS when offloading is enabled.
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.
438648	`outbound enable` not set on bi-directional IPsec policy.
439923	For FG-60E, 12-character FQDN Peer ID causes communication failure.
440615	When `monitor-hold-down-delay` is used in IKEv2 then the value of `monitor-hold-down-delay` has no effect and so once the IKE SA for the primary tunnel is established, it immediately takes the secondary down.

Log & Report

Bug ID	Description
386668	FortiGate sends FortiAnalyzer different time stamps from its disk log.
391013	Some traffic flow does not show in traffic log.

Bug ID	Description
396319	For the `NGFW_vdom`, the application UTM log action is always `PASS` when firewall policy deny the traffic.
409831	Traffic statistic not tally in report.
413778	With long VDOM names, no log is displayed when only one field subtype forward is added to traffic log filter.
417128	Syslog message are missed in FortiGate.

Proxy

Bug ID	Description
414496	URL getting *Blocked - IPS Sensor Triggered*.
415627	After upgrading to 5.6, certificate inspection causes certificate warning.
418193	Some HTTPS sites show *Secure Connection Failed* (static URL filter only flow-based webfilter, certificate inspection).
424362	Multiple crashes of WAD process.
437990	MiTM Proxy mode `HTTPS Interception Weakens TLS Security`.

Router

Bug ID	Description
397087	VRIP cannot be reached on FG-51E when it is acting as VRRP master.
412336	Specific static route on vwl member interface should not be controlled by vwl status.
415366	WAN LLB with IP pools configured for two ISP connections.
424381	TCP sessions are stuck or time out randomly.
434026	SD-WAN health check does not remove route.

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.
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.
411479	The icon used to signify the source of logs when the time range is set to *now* is incorrect.
411645	Drilling down from a root FortiGate to a downstream FortiGate causes an error.
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.
412930	The *Security Audit Event* is not hidden on Security Fabric child nodes.
413189	The bubble chart with FortiAnalyzer view may not be drawn correctly.
413492	Security Fabric topology change can cause high CPU usage by `miglogd` on Security Fabric root.
413742	In Security Fabric topology, the red circle to indicate the root node of the Security Fabric should not be displayed on each child FortiGate.
413912	In Security Fabric topology, the upstream FortiGate can still be displayed when Security Fabric is disabled on a downstream FortiGate.
414147	In Security Fabric topology, the topology cannot be updated after changing the upstream port on a child FortiGate.
414301	Security Fabric topology is not displayed due to js error `Cannot read property 'VDOM' of undefined`.

SLBC

Bug ID	Description
378207	`authd` process causes high CPU usage when only RSSO logging is configured.

Spam

Bug ID	Description
398277	Application scanunit crashes with `signal 6 received`.
408971	Management Traffic is sent out via wrong interface in Virtual WAN Link.
410420	Spam emails are exempted if they are sent in one session.
416790	`(no.x pattern matched)` is not logged when bwl matches envelop `MAIL FROM`.
424443	Client behind FG-60E cannot get bounced mail when sending a spam mail to Hotmail /Outlook.

SSL VPN

Bug ID	Description
304528	SSL VPN Web Mode PKI user might immediately log back in even after logging out.
380974	Possible root cause of SSL VPN fail with `error:0B080074: ..X509_check_private_key:key values mismatch/ApacheSSLSetCertStuff`.
396788	SSL VPN GUI is unable to keep SSO password information for user bookmark.
399784	URL modified incorrectly in a dropdown list in application server.
406028	Citrix with Xenapp 7.x not working via SSL VPN web portal.
408624	SSL VPN certificate UPN+LDAP authentication works only on first policy.
412850	SSL VPN portal redirect fails with a Javascript error.
413758	Auto-generated SSL interface do not associate with `SSLVPN_TUNNEL_ADDR1` for a long name VDOM.
414074	Application with Jira 7.2 and higher does not display properly in SSL VPN web mode.
415543	Request ability to exclude certain services from being created via personal bookmark.
415746	SSO on SSL VPN HTTP bookmark uses OTP instead of password in Auth HTTP header field when user authenticates via TFA.
423415	Incorrectly resolved membership for group members using SSL VPN.
424561	SSL VPN web mode has trouble loading certain page in HTTP/HTTPS bookmark.
433779	RDP bookmark doesn’t work after upgrading to 5.6.

Bug ID	Description
438004	A bookmark having access link to a web page does not work via SSL VPN web mode.
441837, 441854	SSL VPN web mode host-check doesn't work.

System

Bug ID	Description
383126	FG-50E/FG-51E TP mode - STP BPDU forwarding destined to 01:80:c2:00:00:00 stops after warm/cold reboot.
396781	Interface policy cannot block traffic encapsulated in PPPoE.
403572	Fragmentation not working on VLAN with `mtu-override` on NP6.
410463	SNMP is not responding when queried on a loopback IP address with an asymmetric SNMP packet path.
412184	If you use port 4433 for the `admin-port`, `admin-sport`, you cannot access GUI anymore.
412244	Fortitoken Mobile push won't work when VDOM is enabled.
413885	`long-vdom-name` of global setting is disabled after `exe factoryrest2`.
413909, 404337	The *diagnose hardware test system cpu*, *diagnose hardware test cpu model*, and *diagnose hardware test bios* fail to produce a correct hardware report. Affected models: FortiGate / FortiWiFi 30E, 50E, 51E, 52E, 60E, 61E, 80E, 81E, 100E, 100EF, 101E, and 140E series.
414242	Offload not supported on 200E aggregate interfaces.
414482	The pre-allocated size for interface cache and policy cache is not big enough.
415555	IPv6 `ipv6-neighbor-cache` configuration is lost after a reboot or flush command.
416950	NP6 stops process traffic through IPsec tunnel.
417644	When remote wildcard admin with Radius `accprofile-override` is enabled (super admin), restoring config fails on slave.
420150	NTPv3 with authentication enabled fails with error `receive: authentication failed`.
421813	With VDOM enabled, after restoring a VDOM, the members of a zone are removed.

Bug ID	Description
422414	FG-90D + FG-100D modem port not responding.
422755	FG-60D removes session unexpectedly - `memory_tension_drop` increase even though memory usage is very low.
423039	After the upgrade from 5.4.4 to 5.6.0, FortiGate cannot receive public IP with Netgear Aircard 341U.
423375	Some configurations are missing in the output of show full-configuration.
424213	Cluster virtual MAC address is changed to physical port MAC address when ports are assigned on MGMT-VDOM.
434480	Admin user session does not time out.
434823	Firewall system halted when the sniffer is enabled in console.
436211	Kernel conserve mode due to memory leak.
436437	FortiGate cannot apply the FortiClient renew license from FortiGuard server.
437599	ICMP unreachable packet is blocked by transparent FortiGate.
438197	PPPoE connection is disrupted by HA failover/failback.
438944	BPDU frames are not changed in TP mode when one arm is connected to multiple VLANs.
439897	Virtual wire pair on asymmetric environment issue.
440041	DHCPv6 seems to fail when `ip6-mode` is DHCP – failed to assign link-local address.

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.

User

Bug ID	Description
378085	User authentication timeout max setting change.
410901	PKI peer CA search stops on first match based on CA subject name.

Bug ID	Description
412487	*RSSO Endpoint Storage* limits the number of characters to 48.
421456	FortiGate cannot authenticate with Cisco ISE Radius and token.
434849	*Guest User Email Template* cut off when emailed to the recipient.
439760	User name is not visible in logs and on blocking page when using explicit proxy and Kerberos authentication.

VM

Bug ID	Description
414402	`vmtoolsd` continuously crashes.
414811	Restore NIC offload capabilities on FortiGate KVM VM.
416783	FortiGate Image for ESXi loses interface information when `reboot-upon-config-restore` is disabled and a config is restored.
438174	Fortinet VM Product range device detection improved.

VoIP

Bug ID	Description
423437	SIP ALG does not translate all MSRP SEND messages if more than one SEND message is contained within a single packet.

WebProxy

Bug ID	Description
398405	WAD crashes without backtrace - WAF HTTP header matching problem.
406292	After update to 5.4.3 (B1111), WAD sometimes crashes.
415385	Explicit FTP proxy issue on zero file size transfers.
417491	WAD crashes when handling FTP over HTTP traffic.
421092	WAD consuming memory when explicit webproxy is used.
423077	WAD crashed after upgrading from 5.2.10 to 5.4.4 GA release.

Bug ID	Description
423128	Unable to access `www.ch.endress.com` when deep inspection is enabled on explicit-proxy policy.
424208	Expired certificates with valid issuers are treated as untrusted.
438759	TeamViewer not blocked with explicit proxy application control with SSL “deep inspection”.

WiFi

Bug ID	Description
396580	Memory leak and crash reported for `hostapd`.
409110	Web page override login page loads slowly.
413214	Remote APs traffic not working.
413693	WPA_Entreprise with Radius Auth mode fails with VDOM that has a long VDOM name.
417001	Explicit HTTP proxy drops HTTPS connections on WiFi rating failures.
420967	Proxy AV + Proxy WF + SSL Certificate Inspection (Inspect All Ports) results in HTTPS traffic bypassing WiFi.
423020	Regex value changes in the URL filter.
436354	Replace Message Group *Web Filter Block Override* page not working.
438003	Part of APs failed to be managed by FortiGate because `cw_acd` crashed in CMCC portal authentication.

Common Vulnerabilities and Exposures

Bug ID	Description
409913	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2017-3130 Visit https://fortiguard.com/psirt for more information.
414418	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2017-3131 • 2017-3132 • 2017-3133 Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
415416	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2017-7733 Visit https://fortiguard.com/psirt for more information.
416322	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2017-2636 Visit https://fortiguard.com/psirt for more information.
416914	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2016-10229 Visit https://fortiguard.com/psirt for more information.
421539	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2009-3555 Visit https://fortiguard.com/psirt for more information.
422133	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2009-3555 Visit https://fortiguard.com/psirt for more information.
422382	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2018-1352 Visit https://fortiguard.com/psirt for more information.
438599	FortiOS5.6.1 is no longer vulnerable to the following CVE Reference: • 2005-4900 Visit https://fortiguard.com/psirt for more information.
440744	FortiOS 5.6.1 is no longer vulnerable to the following CVE Reference: • 2017-7739 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.6.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
435951	Traffic keeps going through the `DENY` NGFW policy configured with URL category.
441996	No UTM AppCtrl log for signature `Gmail_Attachment.Download` when action is blocked.

Firewall

Bug ID	Description
434959	NGFW policy with App Control policy blocks traffic.

FortiGate 3815D

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

FortiLink

Bug ID	Description
434470	Explicit policy for traffic originating from interface dedicated to FortiLink.
441300	Limited options in FortiLink quarantine stanza to use, giving users no way to trigger the quarantine function.

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.

Bug ID	Description
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. Workaround: disable `switch-controller-dhcp-snooping` on FortiLink VLAN interfaces.
445373	For 802.1X, FortiSwitch port disappeared after upgrading FortiGate from 5.6.0 to 5.6.1 with 802.1X enabled without security-group/user-group.

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.
402507	In physical/logical topology, threat drill down fails and keeps GUI loading unexpectedly.
408100	Log fields are not aligned with columns after drill down on FortiView and Log details.
441835	Drill down a auth-failed wifi client entry in "Failed Authentication" could not display detail logs when CSF enabled.
442238	FortiView VPN map can’t display Google map (199 dialup VPN tunnel).
442367	In *FortiView > Cloud Applications*, when the cloud users column is empty, drill down will not load.

GUI

Bug ID	Description
375383	If the policy includes the *wan-load-balance* interface, the policy list page may receive a javascript error when clicking the search box.
398397	Slowness in accessing *Policy* and *Address* page in GUI after upgrading from 5.2.2 to 5.4.1.
402775	Add multiple ports and port range support in the explicit FTP/web proxy.

Bug ID	Description
403146	Slow GUI *Policy* tab with more than 600 policies.
412401	Incorrect throughput reading in *GUI-System-HA* page.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
454259	The *Policy* list page does not display tooltips for policy comments.

HA

Bug ID	Description
439152	FGSP - standalone config sync - synchronizes BGP neighbor.
441078	The time duration of packet-transporting process stops to pre-master node after HA failover takes too long.
441716	Traffic stops when `load-balance-all` is enabled in active-active HA when `npu_vlink` is used in the path.
436585	Issues with different hardware generation when operating in a HA cluster.

IPsec

Bug ID	Description
416102	Traffic over IPsec VPN gets dropped after two pings when it is getting offloaded to NPU.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FGT does not create webfilter logs.
438858	Synchronized log destination with *Log View* and *FortiView* display source.
441476	Rolled log file is not uploaded to FTP server by `max-log-file-size`.

Proxy

Bug ID	Description
442252	WAD stops forwarding traffic on both transparent proxy and explicit web proxy after IPS test over web proxy.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
409156	In Security Fabric Audit, The unlicensed FDS FortiGate shouldn't be marked *Passed* in *Firmware & Subscriptions*.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the *Device* field.
414013	Log Settings shows `Internal CLI error` when enabling historical FortiView at the same time as disk logging.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.
442808	SSL VPN signal 11 crash on corporate firewall.

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.
436580	`PDQ_ISW_SSE` drops at +/-100K CPS on FG-3700D with FOS 5.4 only.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
437801	FG-30E WAN interface MTU override drop packet issue.
438405	HRX/PKTCHK drops over NP6 with 1.5 Gbps.
439126	Auto-script using diagnose command fails with `Unknown action 0` after rebooting FortiGate.
439553	Virtual wire pair config missing after reboot.
440411	Monitor NP6 IPsec engine status.

Bug ID	Description
440412	SNMP trap for per-CPU usage.
440448	FG-800C will not get IP on the LTE-modem interface using Novatel U620.
441532	Suggest to add SNMP/CLI monitoring capabilities of NP6 session table.

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.