FortiOS - Release Notes

Version 5.6.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

May 27, 2019
FortiOS 5.6.3 Release Notes
01-563-459301-20190527

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-12-05	Initial release.
2017-12-07	Added 443203 to *Resolved Issues*. Added 463211 to *Known Issues*. Moved 452384 from *Known Issues* to *Resolved Issues*. Deleted Internet Explorer version 11 from *Product Integration and Support*.
2017-12-08	Added 443870 to *Resolved Issues*. Added caution to *Upgrade Information > Upgrading to FortiOS 5.6.3*.
2017-12-12	Added *Introduction > Special branch supported models* section.
2017-12-15	Deleted 415380 from *Known Issues*. Added to *Upgrade Information > Upgrading to FortiOS 5.6.3* that you can upgrade from version 5.4.7 to 5.6.3.
2017-12-22	Added 442981 to *Resolved Issues*. Added 456566 to *Known Issues*.
2017-12-29	Added 442800 to *Resolved Issues*. Added 466314 to *Known Issues*. Added caution to *Upgrade Information > Upgrading to FortiOS 5.6.3*.
2018-01-09	Added 454259 to *Resolved Issues*. Moved 364280 to *Special Notices > Using ssh-dss algorithm to log in to FortiGate*.
2018-01-11	Added 364688 and 458880 to *Resolved Issues*. Added 393139 and 424212 to *Known Issues*. Deleted duplicates 422901 and 451456 from *Known Issues*.
2018-01-25	Added 444974 and 445174 to *Resolved Issues*. Moved 461731 from *Known Issues* to *Resolved Issues*. Added *Introduction > Supported models > VXLAN supported models* section.
2018-01-29	Deleted FG-3700DX from *Introduction > Supported models > VXLAN supported models* section. Added 444974 to *Resolved Issues > Common Vulnerabilities and Exposures*.
2018-01-31	Deleted 444974 from *Resolved Issues > Common Vulnerabilities and Exposures* as it's not a CVE issue.

Date	Change Description
2018-02-27	Added 452797 to *Resolved Issues*. Updated 416102 in *Resolved Issues*. Added workaround to 466314 in *Known Issues*. Updated Note in *Upgrade Information > Upgrading to FortiOS 5.6.3*.
2018-03-12	Deleted 455284 from *Known Issues*.
2018-04-02	Updated *Upgrade Information > Upgrading to FortiOS 5.6.3*.
2018-04-27	Added IE 11 to *Product Integration and Support > FortiOS 5.6.3 support > Explicit Web Proxy Browser*.
2018-05-04	Added 477885 to *Known Issues*.
2018-05-22	Updated *Special Notices > Built-in certificate*.
2018-06-18	Deleted 374247, 375036, and 439185 from *Known Issues*.
2018-06-20	Deleted *Upgrade Information > FortiGate-VM64-Azure upgrade*.
2018-11-05	Added 439925 to *Resolved Issues*.
2018-12-21	Added 439469 to *Resolved Issues*.
2019-02-05	Added 297832 to *Known Issues*.
2019-05-27	Deleted 452730 from Resolved Issues.

Introduction

This document provides the following information for FortiOS 5.6.3 build 1547:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.6.3 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-60E-POE, 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-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, 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-3960E, FG-3980E, 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-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-SVM, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM
FortiOS Carrier	FortiOS Carrier 5.6.3 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 5.6.3. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1547.

FG-90E	is released on build 7719.
FG-91E	is released on build 7719.

VXLAN supported models

The following models support VXLAN.

FortiGate	FG-30E, FG-30E-MI, FG-30E-MN, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-MC, FG-60E-MI, FG-60E-POE, FG-60EV, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D
FortiWiFi	FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-MC, FWF-60E-MI, FWF-60EV, FWF-61E
FortiGate Rugged	FGR-30D, FGR-30D-A, FGR-35D
FortiGate VM	FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-NPU, FG-VM64-OPC, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM

Special Notices

Built-in certificate

New FortiGate and FortiWiFi D-series and above are shipped with 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.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.3, 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.

FortiExtender support

Due to OpenSSL updates, FortiOS 5.6.3 cannot manage FortiExtender anymore. If you run FortiOS with FortiExtender, you must use a newer version of FortiExtender such as 3.2.1 or later.

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 5.6.3

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*.

> ⚠ If you are upgrading from version 5.6.1 or 5.6.2, this caution does not apply.
>
> 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.

> ⚠ If you are upgrading from version 5.4.5, 5.4.6, or 5.4.7, the IPsec phase1 `psksecret` setting might be lost. To avoid this, upgrade to 5.6.2 and then to 5.6.3.
>
> If the `psksecret` setting is lost, reconfigure it after upgrading.

> ⚠ After upgrading, if FortiLink mode is enabled, you must manually create an explicit firewall policy to allow RADIUS traffic for 802.1x authentication from the FortiSwitch (such as from the FortiLink interface) to the RADIUS server through the FortiGate.

Security Fabric upgrade

FortiOS 5.6.3 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 5.6.1
- FortiClient 5.6.0
- FortiClient EMS 1.2.2
- FortiAP 5.4.2 and later
- FortiSwitch 3.6.2 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 5.6.3, 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 5.6.2, 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 5.6.3, 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 5.6.3 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 5.6.3 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 5.6.3 support

The following table lists 5.6.3 product integration and support information:

Web Browsers	• Microsoft Edge 38 • 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 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	See important compatibility information in Security Fabric upgrade on page 11. • 5.6.1 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient Mac OS X	See important compatibility information in Security Fabric upgrade on page 11. • 5.6.0 If FortiClient is 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)	• 3.6.2 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 0264 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	• 3.2.1 and later See FortiExtender support on page 9.
AV Engine	• 5.247
IPS Engine	• 3.442
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 FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

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	2334. 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
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

It is recommended to verify the accuracy of the GUID for the software you are using for SSL VPN 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 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 5.6.3. For inquires about a particular bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
441996	No UTM AppCtrl log for signature `Gmail_Attachment.Download` when action is blocked.

DLP

Bug ID	Description
435283	`block-page-status-code` doesn't work for HTTP status code of DLP replacement message.
454112	HIBUN file with `*.exe` extension is detected as `exe` file.

DNS Filter

Bug ID	Description
438834	DNS filter blocks access when rating error occurs, even with `allow request on rating error` enabled.

FIPS-CC

Bug ID	Description
440307	Wildcard certificate support/handling for SAN/CN reference identifiers.

Firewall

Bug ID	Description
449195	DNAT not working for SCTP -Multi-homing Traffic.

FortiCarrier

Bug ID	Description
415496	GTPU sanity drop by gtp-in-gtp checking if GTPU payload has kind of invalid UDP header (IP fragment case).
445321	GTP, 2 cases of protocol anomaly drops to review (status=prohibited).

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.
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.

GUI

Bug ID	Description
365378	Cannot assign `ha-mgmt-interface` IP address in the same subnet as other port from the GUI.
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.
403146	Slow GUI *Policy* tab with more than 600 policies.
409100	Edit admin/user, enable FortiToken mobile, or click send activation email before saving sends empty activation code.
412401	Incorrect throughput reading in *GUI-System-HA* page.
442800	The *Monitor > Firewall User Monitor* page fails to load when *Network > Interfaces > Admission Control > Security Mode* is set to *Captive Portal* and *User Access* is set to *Allow all*.
442981	In the GUI, some HA ports' status are displayed wrong.
450919	IPS sensor with >= 8192 signature entries should not be created from GUI.
454259	The *Policy* list page does not display tooltips for policy comments.

HA

Bug ID	Description
412652	Unexpected behavior seen when one cluster unit has a monitored port down and another cluster unit has ping server issues.
436585	Issues with different hardware generation when operating in a HA cluster.
439152	FGSP - standalone config sync - synchronizes BGP neighbor.
441716	Traffic stops when `load-balance-all` is enabled in active-active HA when `npu_vlink` is used in the path.
442085	After HA failover, the new master unit uses an OSPF MD5 authentication encryption sequence that is lower than the previous sequence number.

Bug ID	Description
442663	No NTP sync and feature license invalid at backup device in FGSP cluster.
442907	Admin password expiry calculation is 1 sec. different on master and slave which causes HA to be out of sync for about 20 mins.
449147	No security database update on slave unit in FGSP environment.
452052	`vcluster2`'s VMAC on VLAN Interface is not persistent after `vcluster1` fails over.
452715	`ha-mgmt-interface` on slave unit is overwritten when backed up and restored.
454347	Ping server penalties are taken into account even when they are not configured in HA settings anymore.
455513	Management VDOMs I/F address on slave is lost or sync'ed with Master's.
461731	HA dedicated management port settings are modified and unreachable after restoring the configuration backup.

IPS

Bug ID	Description
445174	IPS engine crash on some models causes reboot.

IPsec VPN

Bug ID	Description
401847	Half of IPsec tunnels traffic lost 26 minutes after power on a spare 1500D.
416102	Traffic over IPsec VPN gets dropped after two pings when it is getting offloaded to NPU. ⚠ Depending on VPN traffic usage, CPU usage might have a large increase.
441267	FortiGate static remote-gateway can change if peer sends ESP traffic with different IP address.
442671	Set broadcast-forward enable not working for IPsec interface.
445657	FortiOS Traffic Selector narrowing accepts wrong proposal.

Log & Report

Bug ID	Description
422901	Power disruption message when logging with `prof_admin`.
441476	Rolled log file is not uploaded to FTP server by `max-log-file-size`.

Bug ID	Description
443001	Export log field descriptions for documentation.

Proxy

Bug ID	Description
403140	Improve filtering capabilities of LDAP search Explicit Proxy with Kerberos authentication.
435332	Keepalive Exempted HTTPs traffic keeps on kernal and proxy.
439925	Web proxy does not update the WAD user's list when new users log in.
441284	www.nieporet.pl website loads very slowly in proxy mode when AV is applied.
442252	WAD stops forwarding traffic on both transparent proxy and explicit web proxy after IPS test over web proxy.
442328	Replacement message image fails to load.
443870	Incorrect extended master secret (EMS) handling in proxy mode deep-inspection causes SSL connection failure.
444257	After Upgrading from 1466 to 1484 GA, SSL Deep Inspection breaks for many SSL sites using Chrome.
445312	`tcp-timewait-timer` does not have any effect when WAD is running.
445374	Proxies should preserve DSCP flags.
447274	Specific web page fails to load when proxy-based AV profile is enabled on Explicit web proxy policy.

Routing

Bug ID	Description
441506	BGP Aggregate address results in blackhole for incoming traffic.

Security Fabric

Bug ID	Description
409156	In Security Fabric Audit, the unlicensed FDS FortiGate shouldn’t be marked *Passed* in *Firmware & Subscriptions*.

SSL VPN

Bug ID	Description
412850	SSL VPN portal redirect fails with a Javascript error.

Bug ID	Description
443203	In SSL VPN web mode, RDP quick connect fails with domain\username format credentials via NLA.
452797	SSL VPN web portal SSO form data supports dynamic username with prefix and suffix.

System

Bug ID	Description
278660	FGT-AWSONDEMAND is unable to handle FortiCare registration.
290708	`nturbo` may not support CAPWAP traffic.
393006	NPU offloading causes issues with Arista.
404119	FSSO is not enabled when FSSO policy was created.
411415	Update FortiOS API to remove IPS sessions in parallel with firewall sessions.
414811	Restore NIC offload capabilities on FortiGate KVM VM.
420568	`fclicense` daemon has several signal 11 crashes.
422413	Use API monitor to get data for FortiToken list page.
423332	Merge Top3 "Improve GTP Performance" to 5.6 and 5.8.
423508	Traffic from CAPWAP is not offloading on NP6 FortiGate.
437195	GTE - PDP update request should update the associated tunnel even when two TEID's are the same.
437589	Slow throughput on 1000D between 10G and 1G interfaces.
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.
439469	Dropped packets only on the LACP Interface but not on the physicals that is part of the LAG.
440412	Added SNMP trap for per-CPU usage.
440448	FG-800C will not get IP on the LTE-modem interface using Novatel U620.
440564	After clicking the DHCP renew button, the GUI page doesn’t refresh.
440850	Latency noticed with port pair when MAC address flapping between port pair members.
440923	The FortiGate interface DHCP client does not work properly in some situations.
441269	3600C memory leak due to IKED.
441532	Suggest to add SNMP/CLI monitoring capabilities of NP6 session table.

Bug ID	Description
442300	FGT5HD kernel panic on 5.6.0-build 1449.
443019	After running for some time, the FG-30E console keep printing memory leak error messages.
444090	Cannot get SNMP values for NP6 counters.
444974	OSPF protocol implementations may improperly determine LSA recency.
451456	Support DHCP Option 82 on FortiGate DHCP relay - rfc3046.
454939	Virtual-wire-pair config is lost after reboot when using at least one VXLAN interface as member.

Wireless

Bug ID	Description
364688	Packet loss when offloading CAPWAP traffic.
414606	CAPWAP encapsulated DNS traffic not forwarded back to IPsec tunnel.
421239	Tunnel mode SSID not working when FortiAP managed through IPsec VPN with NP6 offloading enabled.
437949	Split tunnel enhancement: `set split-tunneling-acl-path [tunnel | local]`.

Common Vulnerabilities and Exposures

Bug ID	Description
442365	FortiOS 5.6.3 is no longer vulnerable to the following CVE Reference: • 2017-7738 Visit https://fortiguard.com/psirt for more information.
446892	FortiOS 5.6.3 is no longer vulnerable to the following CVE Reference: • 2017-13077 • 2017-13078 • 2017-13079 • 2017-13080 • 2017-13081 Visit https://fortiguard.com/psirt for more information.
452384	FortiOS 5.6.3 is no longer vulnerable to the following CVE Reference: • 2017-14185 Visit https://fortiguard.com/psirt for more information.
453971	FortiOS 5.6.3 is no longer vulnerable to the following CVE Reference: • 2017-14187 Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
456392	FortiOS 5.6.3 is no longer vulnerable to the following CVE Reference: • 2017-13077 Visit https://fortiguard.com/psirt for more information.
458880	FortiOS 5.6.3 is no longer vulnerable to the following CVE Reference: • 2017-14190 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.6.3. 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.
448247	Traffic-shaper in shaping policy does not work for specific application category like as P2P.

Authentication

Bug ID	Description
460229	Existing terminal server sessions overridden with the last TS user that logged in.

AV

Bug ID	Description
446204	The filename of character in Korean shows mismatch encoding type in GUI.

FIPS-CC

Bug ID	Description
463211	When alarm is enabled in FIPS mode, the console hangs and the getty process uses very high CPU usage.

FortiGate-90E/91E

Bug ID	Description
393139	Software switch span doesn't work on this platform.
424212	FG-90E can't receive packets from span ports.

FortiGate 500D

Bug ID	Description
403449	FortiGate 500D has some issue with FINISAR transceiver.

FortiGate 3815D

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

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	HA with FortiLink traffic loss – no virtual MAC.
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* in a hidden way.
462080	FG-300E reboots with kernel panic errors.
477885	FSW Security Policy – RADIUS configuration not pushed to FSW if `source-ip` is specified. Workaround: configure a separate RADIUS server without `source-ip` parameter and use it in the FSW security policy.

FortiView

Bug ID	Description
366627	FortiView Cloud Application may display 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.
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
297832	Administrator with read-write permission on Firewall Configuration is not able to read or write firewall policies. Workaround: use "super_admin" accprofile for administrator.
356174	FortiGuard `updategrp` read-write privilege admin cannot open FortiGuard page.
374844	Should show `ipv6` address when set `ipv6` mode to `pppoe/dhcp` on *GUI > Network > Interfaces*.
375383	If the policy includes the *wan-load-balance* interface, the policy list page may receive a javascript error when clicking the search box.
422413	Use API monitor to get data for FortiToken list page.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
445113	IPS engine 3.428 on Fortigate sometimes cannot detect Psiphon packets that iscan can detect.
446756	Guest user print template can’t display pictures while printing.
451776	Admin GUI has limit of 10 characters for OTP.
456566	In firewall policy list, need to add support for custom sections.
459904	Rogue AP Monitor does not show the *Name* of the AP in the *Detected By* column.

HA

Bug ID	Description
441078	The time duration of packet-transporting process stops to pre-master node after HA failover takes too long.
457554	FortiGate does not send syslog after `ha-mgmt-interface` link goes down and then up.
457877	Packets dropped with TNS session-helper enabled on FGSP cluster.
458320	Cluster uptime was not consistent.
461915	When *standalone config sync* is enabled in FGSP, IPv6 setting of interface is sync’ed.

IPS

Bug ID	Description
443418	User is not listed in quarantine list in case `block duration` value is set long enough.
450693	`ERR_SSL_PROTOCOL_ERROR` when deep scan enabled along with IPS in policy.

IPsec VPN

Bug ID	Description
466314	The IPsec phase1 `psksecret` setting might be lost after upgrading from 5.4.x. Workaround: upgrade to 5.6.2 and then to 5.6.3.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create webfilter logs.
438858	Synchronized log destination with *Log View* and *FortiView* display source.

Proxy

Bug ID	Description
454185	Specific application does not work when deep inspection is enabled.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
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.
441068	SSL VPN unable to connect in tunnel mode, seeing multiple stale sessions for the same user.

System

Bug ID	Description
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
436580	`PDQ_ISW_SSE` drops at +/-100K CPS on FG-3700D with FOS 5.4 only.

Bug ID	Description
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
440411	Monitor NP6 IPsec engine status.
450389	IPv6 problem with neighbor-cache.
457096	FortiGate to FortiManager tunnel (FGFM) using the wrong source IP when multiple paths exist.
459273	Slave worker blade loses local administrator accounts.

VM

Bug ID	Description
441129	Certify FortiGate-VMX v5.6 with NSX v6.3 and vSphere v6.5.

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.