

FortiOS - Release Notes

Version 5.6.8

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 COOKBOOK

<http://cookbook.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



April 25, 2019

FortiOS 5.6.8 Release Notes

01-568-535659-20190425

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported models	5
Special branch supported models	6
VXLAN supported models	6
Special Notices	7
FortiGates in an SLBC cluster can go out of sync after a FortiGuard update	7
Built-in certificate	7
FortiGate and FortiWiFi-92D hardware limitation	8
FG-900D and FG-1000D	8
FortiGate-VM 5.6 for VMware ESXi	8
FortiClient profile changes	9
Use of dedicated management interfaces (mgmt1 and mgmt2)	9
FortiExtender support	9
Using ssh-dss algorithm to log in to FortiGate	9
Using FortiAnalyzer units running older versions	9
BGP metric attribute	10
Upgrade Information	11
Upgrading to FortiOS 5.6.8	11
Security Fabric upgrade	11
FortiClient profiles	12
FortiGate-VM 5.6 for VMware ESXi	12
Downgrading to previous firmware versions	12
Amazon AWS enhanced networking compatibility issue	13
FortiGate VM firmware	13
Firmware image checksums	14
Product Integration and Support	15
FortiOS 5.6.8 support	15
Language support	17
SSL VPN support	17
SSL VPN standalone client	17
SSL VPN web mode	18
SSL VPN host compatibility list	18
Resolved Issues	20
Known Issues	24
Limitations	27
Citrix XenServer limitations	27
Open source XenServer limitations	27

Change Log

Date	Change Description
2019-01-31	Initial release.
2019-02-04	Moved 531575 and 534346 from <i>Known Issues</i> to <i>Resolved Issues</i> . Updated <i>Product Integration and Support > FortiOS 5.6.8 support > Fortinet Single Sign-On (FSSO)</i> to build 0275.
2019-02-14	Added model FGR-30D to <i>Introduction > Supported models</i> . Added 496642 to <i>Resolved Issues > Common Vulnerabilities and Exposures</i> .
2019-02-28	Deleted 503897 from <i>Resolved Issues</i> .
2019-03-04	Added 534442 to <i>Resolved Issues</i> .
2019-04-17	Added 539155 to <i>Known Issues</i> .
2019-04-25	Added 546145 to <i>Known Issues</i> .

Introduction

This document provides the following information for FortiOS 5.6.8 build 1672:

- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Limitations](#)

For FortiOS documentation, see the [Fortinet Document Library](#).

Supported models

FortiOS 5.6.8 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-90E, FG-91E, 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, FG-5001E, FG-5001E1
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-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-SVM, FG-VMX, FG-VM64-XEN
FortiOS Carrier	FortiOS Carrier 5.6.8 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 5.6.8. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1672.

FG-60E-DSL	is released on build 4211.
FG-60E-DSLJ	is released on build 4211.
FWF-60E-DSL	is released on build 4211.
FWF-60E-DSLJ	is released on build 4211.

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-DLS, 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, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, 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-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, 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, FOS-VM64-XEN

Special Notices

FortiGates in an SLBC cluster can go out of sync after a FortiGuard update

When operating normally, FortiOS uses a collection of CAs (called a CA bundle) for various certificate-related functions. FortiOS normally gets the latest CA bundle from FortiGuard.

FortiOS firmware images come with their own CA bundle. Immediately after a firmware upgrade, all of the FortiGates in a Session-aware Load Balancing Cluster (SLBC) will have the CA bundle that comes with the firmware image. When the first automatic or manual FortiGuard update occurs, the primary FortiGate in the SLBC downloads the latest CA bundle from FortiGuard and synchronizes it to the other FortiGates in the cluster. Due to a known issue with FortiOS 5.6.7 and earlier, this synchronization step may fail, resulting in a synchronization problem with the cluster.

You can avoid this issue by using the following steps to upgrade the firmware of the FortiGates in an SLBC cluster, perform a FortiGuard update, and manually re-synchronize the configuration:

1. Log into the primary FortiGate, and enter the following command to disable graceful-upgrade:

```
config system elbc
    set graceful-upgrade disable
end
```
2. Use the normal firmware upgrade procedure to upgrade the SLBC firmware.
3. After all of the FortiGates have restarted and joined the cluster, log into the primary FortiGate, and use the `diagnose sys confsync status` command to verify that the primary FortiGate can communicate with all of the FortiGates in the cluster.
4. Enter `diagnose autoupdate versions | grep -A2 'Bundle'` to check the version of CA bundle on the primary FortiGate.
For FOS v5.6.7, the bundle version should be 1.00012.
5. Start a FortiGuard update on the primary FortiGate.
For example, use the `execute update-now` command.
6. Wait a few minutes, then enter `diagnose autoupdate versions | grep -A2 'Bundle'` to verify that a new CA bundle has been installed.
7. Back up the configuration of the primary FortiGate.
8. Restore the configuration of the primary FortiGate.
The primary FortiGate should synchronize this configuration to all of the other FortiGates in the cluster. After a few minutes, all of the FortiGates in the cluster should restart and their configurations should be synchronized.
9. Use the `diagnose sys confsync status` command to verify that the cluster is synchronized.

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 5.6.8, 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 5.6.8 cannot manage FortiExtender 3.2.0 or earlier. If you run FortiOS 5.6.8 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.

Using FortiAnalyzer units running older versions

When using FortiOS 5.6.8 with FortiAnalyzer units running 5.6.5 or lower, FortiAnalyzer might report increased bandwidth and session counts if there are sessions that last longer than two minutes.

For accurate bandwidth and session counts, upgrade the FortiAnalyzer unit to 5.6.6 or higher, or 6.0.2 or higher.

BGP metric attribute

The BGP metric attribute does not work when manipulated by `route-map`. For self-generated default origin route, do not use `route-map-out`. Use `default-originate-routemap` instead. For example:

```
config router bgp
config neighbor
  edit "1.1.1.1"
    set capability-graceful-restart enable
    set capability-default-originate enable
    set ebgp-enforce-multihop enable
    set remote-as 65001
    set route-map-out "Default"           (delete this line)
    set default-originate-routemap "Default" (add this line)
  next
end
```

You must also delete `match-ip-address`. For example:

```
config router route-map
  edit "Default"
    config rule
      edit 1
        set match-ip-address "0.0.0.0/0" (delete this line)
        set set-metric 100
      next
    end
  end
end
```

Upgrade Information

Upgrading to FortiOS 5.6.8

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 5.6.2, 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.



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 5.6.8 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 5.6.8, 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 5.6.8, 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 5.6.8 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 5.6.8 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 5.6.8 support

The following table lists 5.6.8 product integration and support information:

Web Browsers	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 . <ul style="list-style-type: none">• 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 . <ul style="list-style-type: none">• 5.6.0 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient iOS	<ul style="list-style-type: none">• 5.4.3 and later
FortiClient Android and FortiClient VPN Android	<ul style="list-style-type: none">• 5.4.1 and later

FortiAP	<ul style="list-style-type: none"> • 5.4.2 and later • 5.6.0
FortiAP-S	<ul style="list-style-type: none"> • 5.4.3 and later • 5.6.0
FortiSwitch OS (FortiLink support)	<ul style="list-style-type: none"> • 3.6.2 and later
FortiController	<ul style="list-style-type: none"> • 5.2.5 and later <p>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C.</p>
FortiSandbox	<ul style="list-style-type: none"> • 2.3.3 and later
Fortinet Single Sign-On (FSSO)	<ul style="list-style-type: none"> • 5.0 build 0275 and later (needed for FSSO agent support OU in group filters) <ul style="list-style-type: none"> • 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 <p>FSSO does not currently support IPv6.</p>
FortiExtender	<ul style="list-style-type: none"> • 3.2.1 and later <p>See FortiExtender support on page 9.</p>
AV Engine	5.00361
IPS Engine	3.00539
Virtualization Environments	
Citrix	<ul style="list-style-type: none"> • XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	<ul style="list-style-type: none"> • RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	<ul style="list-style-type: none"> • Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	<ul style="list-style-type: none"> • XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	<ul style="list-style-type: none"> • ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
 <p>FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.</p>	

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

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 Internet Explorer version 11
Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	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 5.6.8. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Explicit Proxy

Bug ID	Description
477289	Proxy is unexpectedly sending FIN packet (FTP over HTTP traffic).
521344	Explicit FTP proxy doesn't work with second IP address.

Firewall

Bug ID	Description
441176	SNMP trap failed to send when LDB real server is down.
479577	Firewall policy should not allow to config <code>dstaddr</code> to "any" which doesn't exist.
492034	Traffic not matching expected sessions and getting denied.
525995	Session marked dirty when routing table updated for route which is not related to the session.

GUI

Bug ID	Description
516295	<i>Error connecting to FortiCloud</i> message while trying to access Forticloud Reports in GUI.
525666	Deleting an object in a non-root VDOM via Reference column deletes the related ID object in the root VDOM.

HA

Bug ID	Description
488383	Cluster fails to sync after adding a new VDOM and rebooting with switch-controller disabled.
494029	After failover, cannot connect to management-IP of backup device.
517537	Slave out-of-sync. Unable to log into slave unit.
525182	WLAN guest user in VDOM makes the cluster out of sync.

IPsec VPN

Bug ID	Description
493918	Memory leak with IKED.

Log & Report

Bug ID	Description
477393	Negative values in 'Load Balance' monitor logs.

Proxy and WebProxy

Bug ID	Description
470407	IPv6-Happy-Eyeballs-Mechanism not working with proxy-based Webfilter-Profile.
491675	FTP Server is not accessible when AV profile is set to proxy based inspection.
512936	SSL certificate inspection in proxy mode doesn't use CN from Valid Certificate for categorization when SNI is not present.
526667	FGT doesn't forward Request:port command after 0byte file transmission.
531575	Website access failure due to OCSP check in WAD + Deep SSL inspection.
534346	WAD memory leak on OCSP certificate caching.
534442	WAD memory still increasing after upgrade to 5.6.7 by 'malloc info'.

Routing

Bug ID	Description
518655	IPv6 doesn't respond to neighbor solicitation request.

SSL VPN

Bug ID	Description
500901	SSL VPN web portal connect to FMG (5.6.3) unable to view Managed devices and policy packages.
518406	Unable to load WebPage through SSL VPN webmode.
523647	Search result gives empty output upon accessing the url <https://ieeexplore.ieee.org> via SSL VPN bookmark.
530833	Synology NAS login page stuck after login when accessing by SSL VPN Web portal.

Switch Controller

Bug ID	Description
525450	Managed FSWs details always opened at top of screen.

System

Bug ID	Description
370151	CPU doesn't remove dirty flag when returns session back to NP6.
461370	Auto MDIX does not work when interface is set to 10full/100full. It only works when interface is set to auto.
466805	Adding USB Host devices to a virtual machine connected by USB to FortiGate 500D causes the units to restart in loop.
482497	Running <i>diagnose npu np6lite session</i> in FG-201E results in high CPU and system instability.
495378	Port2 goes down after running for right days on FG-800D.
508304	IP is not updating in DDNS with 60D models.
513419	High CPU on some cores of CPU & packet drops around 2-3%.
519246	<code>ipmc_sensord</code> process not checking sensors due to pending jobs.
519493	If remote-side change systemID, only one port goes down, the other remains up.
526252	High memory caused by updated daemon.
524422	Merge <code>br_6-0_sp</code> back to 6.0 and 6.2.
524915	5.6 FortiOS replies with wrong numbers for SNMP <code>ifSpeed</code> and <code>ifHighSpeed</code> OIDs when interface is down.
526168	SLBC: System went into out-of-sync after FortiGuard update.
533287	FortiGate lost VLAN tag when using virtual wire pair.

User and Device

Bug ID	Description
437117	Single Sign-on, multiple FSSO polling servers with the same AD (LDAP) server, cannot select the same user or group.
525929	LDAPS requests fail with <code>fnbamd stop</code> error "Not enough bytes". LDAP works fine. Additional timeout observed.

VM

Bug ID	Description
528405	FortiMeter Consumption is not accurate.

Common Vulnerabilities and Exposures

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

Bug ID	Description
452730	FortiOS 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2017-14186
495090	FortiOS 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-13366
496642	FortiOS5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-13371
502940	FortiOS 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-13374
529353	FortiOS 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-13380
529377	FortiOS 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-13379
529712	FortiOS 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-13381

Known Issues

The following issues have been identified in version 5.6.8. For inquiries 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.

Firewall

Bug ID	Description
546145	If the firewall policy includes a nonexistent ISDB ID on updated ISDB version, the firewall policy is not read and reflected.

FortiGate-90E/91E

Bug ID	Description
393139	Software switch span doesn't work on this platform.

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 FortiSwitch 3.4.2 b192.

FortiView

Bug ID	Description
366627	FortiView Cloud Application may display incorrect drill down <i>File and Session</i> list in the <i>Applications View</i> .
368644	<i>Physical Topology: Physical Connection</i> 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.

GUI

Bug ID	Description
356174	FortiGuard <code>updategrp</code> read-write privilege admin cannot open FortiGuard page.
374844	Should show <code>ipv6</code> address when set <code>ipv6</code> mode to <code>pppoe/dhcp</code> on <i>GUI > Network > Interfaces</i> .
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.
451776	Admin GUI has limit of 10 characters for OTP.

HA

Bug ID	Description
481943	Green checkmarks indicating HA sync status on GUI only appear beside virtual cluster 1.
539155	HA master does not send SNMP trap when plugging cable into interface that is set as <code>ha-mgmt-interfaces</code> .

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create webfilter logs.

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 <i>Device</i> field.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.

System

Bug ID	Description
295292	If <code>private-data-encryption</code> is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
436580	<code>PDQ_ISW_SSE</code> 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.
440411	Monitor NP6 IPsec engine status.
457096	FortiGate to FortiManager tunnel (FGFM) using the wrong source IP when multiple paths exist.
464873	RADIUS COA Disconnect-ACK message ignore RADIUS server <code>source-ip</code> setting.

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:

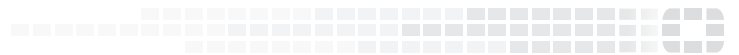
- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
 - XVA (recommended)
 - VHD
 - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require 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.



FORTINET[®]



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.