FortiOS - Release Notes

Version 5.6.11

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: techdoc@fortinet.com

April 9, 2020
FortiOS 5.6.11 Release Notes
01-5611-574176-20200409

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-08-15	Initial release.
2019-08-22	Updated *Common Vulnerabilities and Exposures* in *Resolved Issues*.
2019-09-11	Updated Fortinet Single Sign-On (FSSO) support.
2019-10-28	Deleted *Common vulnerabilities and exposures* in *Special Notices*.
2019-11-18	Changed 555805 to 582569 in *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2020-04-09	Added 576646 to *Known Issues*.

Introduction

This document provides the following information for FortiOS 5.6.11 build 1700:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.6.11 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-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-SVM, FG-VMX, FG-VM64-XEN
FortiOS Carrier	FortiOS Carrier 5.6.11 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 5.6.11. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1700.

FG-60E-DSL	is released on build 4263.
FG-60E-DSLJ	is released on build 4263.
FWF-60E-DSL	is released on build 4263.
FWF-60E-DSLJ	is released on build 4263.
FG-VM64-AZURE	is released on build 6024.
FG-VM64-AZUREONDEMAND	is released on build 6024.

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 5.6.11, 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 5.6.11 cannot manage FortiExtender 3.2.0 or earlier. If you run FortiOS 5.6.11 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 5.6.11 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
```

Changes in tablesize

Maximum number of webfilter profiles

For platforms below 40C, the maximum number of webfilter profiles per VDOM has increased from 10 to 32.

For platforms 40C and above, the maximum number of webfilter profiles per VDOM has increased from 32 to 128.

Firewall address

The maximum firewall address object is increased from 5000 to 10000 for the following platforms:

- FG-70D
- FG-70DP
- FG-80E
- FG-80EP
- FG-81E
- FG-81EP
- FG-WF81CM
- FG-82C
- FG-90D
- FG-90DP
- FGR-90D
- FG-WF90D
- FG-WF90DP
- FG-90E
- FG-91E
- FG-92D
- FG-WF92D
- FG-94DP
- FG-98DP

Upgrade Information

Upgrading to FortiOS 5.6.11

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 5.6.11 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 5.6.11, 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 5.6.11, 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 5.6.11 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 5.6.11 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 5.6.11 support

The following table lists 5.6.11 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 13. 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 13. 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 13. • 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 13. • 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 0281 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2008 Core
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExtender	• 3.2.1 and later See FortiExtender support on page 10.
AV Engine	5.00361
IPS Engine	3.00551
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later

VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5  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 (32-bit & 64-bit)	2336. Download from the Fortinet Developer Network https://fndn.fortinet.net.

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

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

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

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 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

Operating System	Web Browser
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 https://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 5.6.11. For inquires about a particular bug, please contact Customer Service & Support.

Anti-Spam

Bug ID	Description
477496	Unable to add email wildcard to black/white list GUI in Anti-Spam profile.

AntiVirus

Bug ID	Description
569143	CIFS AV flow mode allows malware which has been blocked by HTTP.

Application Control

Bug ID	Description
499598	Application Control with SSL does not check SNI against server certificate.
558380	Application Control does not detect application with `webproxy-forward-server`.
561843	Application Control unscans the traffic to forward to upstream proxy.
562832	Application Control `HTTP.BROWSER_Firefox` is not blocking Facebook and some other sites.

DNS Filter

Bug ID	Description
525068	No need to resolve safe search FQDN if not used.

Explicit Proxy

Bug ID	Description
482916	WAD crash with signal 6.
533838	WAD re-signs valid web sites with untrusted CA certificate.
560076	SSL deep inspection not performed on certain sites.

Firewall

Bug ID	Description
543637	Cannot filter policy by multiple IDs.
557777	Policy ID filter not working for Single Policy ID.

FortiView

Bug ID	Description
552339	In FortiView GUI > All Sessions page, the filter is not working.

GUI

Bug ID	Description
477493	GUI fails to read correct Last Used time for firewall policy.
537550	HTTPSD uses high CPU when accessing GUI network interfaces.
552038	Routing monitor network filter does not filter subnets after upgrade.

HA

Bug ID	Description
518717	MTU of session-sync-dev does not come into effect.
518964	Slowness when adding or removing member from address group via SSH.
519266	FGT-HA does not fail over when pingserver is down the second time.
536520	GTP Tunnel States are not synced on subordinate unit after a reboot.
538289	Old master keeps forwarding traffic after failover.
541224	Network loop over virtual-wire-pair in HA mode if running diagnose `sys ha reset-uptime`.
551995	SCTP sessions affected after upgrade and failover.
552329	NP6 sessions dropped after any change in GUI.
574564	In HA setup, with uninterrupted upgrade option enabled, some signature DBs might be damaged if upgrading from 5.6.9 and earlier to 5.6.10.

Intrusion Prevention

Bug ID	Description
537571	IPS/AV not forwarding return traffic back to clients.

Bug ID	Description
553262	TCP connections through IPsec (bound to loopback) do not work when IPS offload is enabled to NTurbo.
556538	Enabling IPS on IPv4 policy impacting HTTPS traffic over the site to site VPN using PPOE for internal servers.

IPsec VPN

Bug ID	Description
473609	IPsec gateway not matching for PKI user when there is a DC field in the Client Certificate.
522727	Dialup IPsec hardware acceleration drops.
537450	Site-to-site VPN policy based - with DDNS destination fails to connect.
553759	ESP packets are sent to the wrong MAC after a routing change when IPsec SA is offloaded.
568630	`iked` crashes frequently with signal 11.

Log & Report

Bug ID	Description
521020	VPN usage duration days in local report is not correct.
565216	Memory of `miglogd` increases and enters conserve mode.

Proxy

Bug ID	Description
534118	Active SSH sessions to a remote servers are dropped exactly when the `session-ttl` expires.
537183	Removed default `ssl-exempt` entries page show empty.
544517	WAD process crashing and affecting HTTP/HTTPS traffic.
545964	FortiManager sends requests to FortiGate to collect proxy policy hit_count/bytes, and the response from FortiGate misses the `uuid` attribute.

Routing

Bug ID	Description
480174	FortiGate cannot accept passwords starting with `0x` in certain situations (interpreted as HEX).
503686	Application PDMD crashes.

Bug ID	Description
511203	When using policy route for IPv6, NAT64 does not work.
528465	GRE tunnel does not come up.
536986	IPv6 routing failed to choose lower priority route when output interface is specified.
537110	BGP/BFD packets marked as CS0.
538151	NSM crashes during dev and QA test.
539982	Multicast fails after failover from another interface.
557787	Although the routing table was changed in IPv6 network, the offloaded communication stopped.

SSL VPN

Bug ID	Description
513572	FortiGate not sending `Framed-IP-Address` attribute for SSL VPN tunnel in RADIUS accounting packet.
523717	Dropdown list cannot get expanded through bookmarks (SSL VPN).
525106	HTML PABX Admin Console not working correctly in SSL VPN mode.
527348	JavaScript script is not available when connecting using SSL VPN web mode.
527476	Update from web mode fails for SharePoint page using MS NLB.
528289	SSL VPN crashes when it receives HTTP request with header "X-Forwarded-For" because of the wrong use of `sslvpn_ap_pstrcat`.
532261	SSL VPN web mode RDP connection not working when security set to NLA.
532921	Abnormal work of `mac-addr-check` in function SSL VPN.
533008	SSL web mode is not modifying links on certain web pages.
534728	Unable to get dropdown menu from internal server via SSL VPN web mode connection.
538904	Unable to receive SSL tunnel IP address.
546161	TX packet drops on ssl.root interface.
546187	SSL VPN login auth times out if primary RADIUS server becomes unavailable.
551535	HTTP 302 redirection is not parsed by SSL VPN proxy (web mode / bookmark).
556657	Internal website not working through SSL VPN Web mode.
569030	SSL VPN tunnel mode can only add spit tunneling of user's policy with groups and its users in different SSL VPN policies.

System

Bug ID	Description
471690	Email Service > UserName is not enough for longer UserID. it gets truncated and causes authentication failure.
492655	DNSproxy does not seem to update link-monitor module.
493128	`bcm.user` always takes nearly 70% CPU after running Nturbo over IPsec script.
493843	SNMPD's debug messages reveal source code function names.
505522	Intermittent failure of DHCP address assignment.
522973	System reboots due to a kernel panic.
527868	SLBC FortiOS should prevent change of default management VDOM.
529932	Primary DNS server is not queried even after 30 seconds.
533214	After executing shutdown, FGT90E keeps responding to ICMP requests.
537989	Kernel static route randomly lost.
539444	5001D blade rebooted on its own due to kernel panic.
540062	Kernel panic after upgrade from 5.6.7 to 5.6.8.
541243	DHCP option doesn't include all NTP servers.
541527	Changing the order of VDOM in system admin when connected with TACACS+ wildcard admin is not propagated to other blades.
542441	SNMP monitoring of the implicit deny policy not possible.
543054	Setting alias or changing allowed access to aggregate link moves the state from down to up for a few seconds.
545717	USB Modem Huawei E173u-2 not working on FortiGate 60E device.
546169	DHCPD is using more memory on the slave unit than the active unit.
546464	DHCP not working properly with macOS when proxy `arp` is enabled/configured.
546874	Increase `firewall.address` tablesize for 80-90 series.
547720	FortiGate does not support DH 1024 bits as SSH server.
550433	FGT-5001D/B1672: `/tmp/fcp_rt_dump` file lost some IPsec VPN router info after modified IPsec VPN static router setting.
553326	Kernel panic on 3700D running 5.6.8.
554099	Can't poll SNMP v3 statistics for BGP when `ha-direct` is enabled under SNMP user.
557798	High memory utilization caused by `authd` and `wad` process.

Bug ID	Description
560686	4x10G split-port does not work on FG3700D rev 2.
565955	Possible memory leak with IPS engine on FG-1500D.

Upgrade

Bug ID	Description
530793	`config-error-log` shows after upgrade from v5.6.6 to v5.6.7.

User and Device

Bug ID	Description
518129	FSSO failover is not graceful.
545074	Unable to login into FortiGate GUI with Yubikey. CLI works as expected.
558428	When all groups are included in a registry string that contains more than or equal to 16384 characters, the groups cannot be synchronized.
569434	Recurring conflicts between TS-Agent type FSSO sessions and regular FSSO sessions.

VM

Bug ID	Description
484540	FOS VM serial number changes during firmware upgrade.

VoIP

Bug ID	Description
510233	FortiGate VoIP handling.

Web Filter

Bug ID	Description
504239	Signal 11 crash on b0161.
518433	FGT D series number of web filter profiles decreased globally.
540902	VDOM is replying with TCP ACK 0.
544598	Invalid hostname return on GUI when static URL is defined.
562869	Web filter blocks connection.

WiFi Controller

Bug ID	Description
484667	Add support to update `Fortinet_Wifi` certificate through FGD.
530328	CAPWAP traffic dropped when offloaded if packets are fragmented.
556022	`wifi-certificate` settings becomes empty and `eap_proxy` is killed after deleting `ca_bundle` package and rebooting FortiGate.

Common Vulnerabilities and Exposures

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

Bug ID	Description
395544	FortiOS 5.6.11 is no longer vulnerable to the following CVE Reference: • CVE-2017-17544
529719	FortiOS 5.6.11 is no longer vulnerable to the following CVE Reference: • CVE-2018-13383
529745	FortiOS 5.6.11 is no longer vulnerable to the following CVE Reference: • CVE-2018-13382
532730	FortiOS 5.6.11 is no longer vulnerable to the following CVE Reference: • CVE-2019-6693
539553	FortiOS 5.6.11 is no longer vulnerable to the following CVE Reference: • CVE-2019-5586
548154	FortiOS 5.6.11 is no longer vulnerable to the following CVE Reference: • CVE-2019-3855 • CVE-2019-3856 • CVE-2019-3857 • CVE-2019-3858 • CVE-2019-3859 • CVE-2019-3860 • CVE-2019-3861 • CVE-2019-3862 • CVE-2019-3863
582569	FortiOS 5.6.11 is no longer vulnerable to the following CVE Reference: • CVE-2019-5593

Known Issues

The following issues have been identified in version 5.6.11. 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.

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 ForiSwitch 3.4.2 b192.

FortiView

Bug ID	Description
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.

GUI

Bug ID	Description
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*.
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.

Log & Report

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

Routing

Bug ID	Description
576646	Dead `health-check` cannot recover until restarting lnkmtd daemon.

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.

SSL VPN

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

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.
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 `source-ip` setting.

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.