FortiOS - Release Notes

Version 6.0.9

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

January 29, 2020
FortiOS 6.0.9 Release Notes
01-607-598203-20200129

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-01-22	Initial release.
2020-01-29	Removed 577643 from *Resolved Issues* > *Common Vulnerabilities and Exposures*.

Introduction

This document provides the following information for FortiOS 6.0.9 build 0335:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.9 supports the following models.

FortiGate	FG-30D, FG-30D-POE, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, 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-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3400E, FG-3401E, FG3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN, FG-VM64-GCP, FG-VM64-OPC, FG-VM64-GCPONDEMAND
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 6.0.9 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 6.0.9. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0335.

FG-30E-MG	is released on build 5428.
FG-60F	is released on build 6665.
FG-61F	is released on build 6665.
FG-100F	is released on build 6665.
FG-101F	is released on build 6665.
FG-1100E	is released on build 6664.
FG-1101E	is released on build 6664.
FG-2200E	is released on build 6669.
FG-2201E	is released on build 6669.
FG-3300E	is released on build 6669.
FG-3301E	is released on build 6669.
FG-VM64-AZURE	is released on build 5427.
FG-VM64-AZUREONDEMAND	is released on build 5427.
FG-VM64-RAXONDEMAND	is released on build 8649.

Special Notices

WAN optimization and web caching functions

WAN optimization and web caching functions are removed from 60D and 90D series platforms, starting from 6.0.0 due to their limited disk size. Platforms affected are:

- FGT-60D
- FGT-60D-POE
- FWF-60D
- FWF-60D-POE
- FGT-90D
- FGT-90D-POE
- FWF-90D
- FWF-90D-POE
- FGT-94D-POE

Upon upgrading from 5.6 patches to 6.0.0, `diagnose debug config-error-log read` will show command parse error about `wanopt` and `webcache` settings.

FortiGuard Security Rating Service

Not all FortiGate models can support running the FortiGuard Security Rating Service as a Fabric "root" device. The following FortiGate platforms can run the FortiGuard Security Rating Service when added to an existing Fortinet Security Fabric managed by a supported FortiGate model:

FGR-30D-A	FGT-30D	FGT-70D	FWF-30E-MN
FGR-30D	FGT-30D-POE	FGT-70D-POE	FWF-50E-2R
FGR-35D	FGT-30E	FGT-90D	FWF-50E
FGR-60D	FGT-30E-MI	FGT-90D-POE	FWF-51E

FGR-90D	FGT-30E-MN	FGT-94D-POE	FWF-60D
FGT-200D	FGT-50E	FGT-98D-POE	FWF-60D-POE
FGT-200D-POE	FGT-51E	FWF-30D	FWF-90D
FGT-240D	FGT-52E	FWF-30D-POE	FWF-90D-POE
FGT-240D-POE	FGT-60D	FWF-30E	FWF-92D
FGT-280D-POE	FGT-60D-POE	FWF-30E-MI	

Using FortiManager as a FortiGuard server

If you use FortiManager as a FortiGuard server, and you configure the FortiGate to use a secure connection to FortiManager, you must use HTTPS with port 8888. HTTPS with port 53 is not supported.

Built-in certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate and FortiWiFi-92D hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

FortiClient profile changes

With introduction of the Fortinet Security Fabric, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

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

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Using FortiAnalyzer units running older versions

When using FortiOS 6.0.9 with FortiAnalyzer units running 5.6.5 or lower, or 6.0.0-6.0.2, 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 the latest version.

Changes in Table Size

Bug ID	Description
599271	Except for desktop models, all other platforms' table size of VIP real servers are increased as follows: • 1U platforms increased from 8 to 16 • 2U platforms increased from 32 to 64 • High-end platforms increased from 32 to 256

Upgrade Information

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*.

FortiGuard protocol and port number

Fortinet has updated the protocol that is used between the FortiGate unit and FortiGuard. Please read the section under *Resolved Issues* > *Common Vulnerabilities and Exposures*. Upon upgrading to a patched version of FortiOS, customers must manually change the protocol and port used for connecting to FortiGuard.

```
config system fortiguard
    set protocol https
    set port 8888
end
```

Once the FortiGate is upgraded to a patched version, any factory reset will change the default FortiGuard settings to those above—protocol HTTPS and port 8888.

Fortinet Security Fabric upgrade

FortiOS 6.0.9 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.0.0 and later
- FortiClient 6.0.0 and later
- FortiClient EMS 6.0.0 and later
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.4 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*.

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.0.9. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.9 and some running 5.6.x.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.0.9 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.0.9 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

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 6.0.9 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 6.0.9 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*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

Product Integration and Support

The following table lists FortiOS 6.0.9 product integration and support information:

Web Browsers	• Microsoft Edge 44 • Mozilla Firefox version 66 • Google Chrome version 73 • Apple Safari version 12.1 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 41 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 59 • Google Chrome version 65 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in . 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 . For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.0.0 See important compatibility information in Fortinet Security Fabric upgrade on page 12. If you're upgrading both FortiOS and FortiClient from 5.6 to 6.0, upgrade FortiClient first to avoid compatibility issues. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 5.6.0 and later
FortiClient Android and FortiClient VPN Android	• 5.4.2 and later
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 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 0287 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

FortiExtender	• 3.3.2, 4.0.0
AV Engine	• 6.00027
IPS Engine	• 4.00052
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, 6.5, and 6.7
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)	Mozilla Firefox version 66 Google Chrome version 73
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 66 Google Chrome version 73
Linux Ubuntu 16.04 / 18.04 (32-bit & 64-bit)	Mozilla Firefox version 66
MacOS High Sierra 10.13.6	Apple Safari version 12 Mozilla Firefox version 66 Google Chrome version 72
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

SSL VPN host compatibility list

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

Supported Microsoft Windows XP antivirus and firewall software

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

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved Issues

The following issues have been fixed in version 6.0.9. For inquires about a particular bug, please contact Customer Service & Support.

Data Leak Prevention

Bug ID	Description
591178	WAD fails to determine the correct file name when downloading a file from Nextcloud.

DNS Filter

Bug ID	Description
561297	DNS filtering does not perform well on the zone transfer when a large DNS zone's AXFR response consists of one or more messages.
563441	7K DNS filter breaking DNS zone transfer.

Explicit Proxy

Bug ID	Description
578098	Unwanted traffic log generated for firewall policy with web filter profile as `MonitorAll`.
594598	Enabling proxy policies (+400) increases memory by 30% and up to 80% total.

Firewall

Bug ID	Description
535303	Address page takes more than 15 seconds to load with certain configurations.

FortiView

Bug ID	Description
542154	Custom admin is unable to load FortiView when VDOMs or FortiCloud logging are enabled.
556178	*FortiView* > *Sources* historical view sometimes cannot retrieve data from FortiCloud.

GUI

Bug ID	Description
486230	GUI on FG-3800D with 5.6.3 is very slow for configurations with numerous policies.
493704	While accessing the FortiGate page, PC browser memory usage keeps spiking and finally PC hangs.
543260	When modifying the g-default web filter, access denied error message appears.
545443	GUI is slow in FG-300D, FG-500D, FG-600D, FG-1000D, and FG-1200D with a high number of firewall policies.
546580	Should not be able to unset user or user group on an SSL VPN policy when inline editing the source column in the policy list.
556397	IP pools in SSL VPN settings are overwritten when SSL VPN settings are modified in the GUI.
559866	When sending CSF proxied request, segfault happens (httpsd crashes) if FortiExplorer accesses root FortiGate via the management tunnel.
575592	IP pool and tunnel mode settings in `config vpn ssl web portal` are overwritten when SSL VPN settings are modified in the GUI.
593624	GUI behavior is different with local user using super admin profile and TACACS user using super admin profile.

HA

Bug ID	Description
523582	`ha-mgmt` gateway IP gets synced from the master to slave after restoring configurations.
530215	`application hasync` returns "*** signal 11 (Segmentation fault) received ***".
557277	FGSP configured with `standalone-config-sync` will sync the FortiAnalyzer source IP configuration to the slave.
560107	Cluster upgrade from 5.6.7 build 1653 to SB 5.6.8 build 3667 takes longer than normal.

Bug ID	Description
576638	HA cluster GUI change does not send logs to the slave immediately.
585348	`default-gateway` injected by `dynamic-gateway` on PPP interface deleted by other interface down.

Intrusion Prevention

Bug ID	Description
567923	Receiving IPS engine application crash messages.
601944	IPS engine 4.045 (FG-2000E with FOS 6.0.6) signal 14 crash occurred.

IPsec VPN

Bug ID	Description
550333	In an ADVPN spoke with one interface connecting to two hubs, the shortcut created on receiver side matches to the wrong phase 1.
575477	IKED memory leak.
589096	In IPsec after HA failover, performance regression and IKESAs are lost.

Log & Report

Bug ID	Description
493886	`reportd` is sometimes stuck at 99% CPU usage.
527991	Add CLI setting to configure timeout value when connecting to FortiGate Cloud. Enable `async_log` retrieval from FortiGate Cloud.
565505	`miglogd` high CPU utilization.
586038	FortiOS 6.0.6 reports too long VPN tunnel durations in local report.
596278	`sentdelta` and `rcvddelta` showing 0 if syslog format is set to CSV.
599860	When `logtraffic` is set to `all`, existing sessions cannot change the egress interfaces when the routing table is updated with a new outgoing interface.

Proxy

Bug ID	Description
525328	External resource does not support no content length.
566859	In WAD conserve mode 5.6.8, `max_blocks` value is high on some workers.
573028	WAD crash causing traffic interruption.
579400	High CPU with `authd` process caused by WAD paring multiple line content-encoding error and IPC broken between `wad` and `authd`.

REST API

Bug ID	Description
587470	REST API to support revision flag.

Routing

Bug ID	Description
581488	BGP Confederation router sending incorrect AS to neighbor group routers.
584394	VRRP on LAG cannot forward packet after `vrrp-virtual-mac` is enabled.
587198	After failover/recovery of link, E2 route with non-zero forward address recurses to itself as a next hope.
592599	FortiGate sends malformed OSPFv3 LSAReq/LSAck packets on interfaces with MTU = 9k.
595937	PPPoE interface bandwidth is mistakenly calculated as 0 in SD-WAN.
598665	BGP route is in routing table but not in FIB (kernel routing table).

Security Fabric

Bug ID	Description
583107	The *Access Layer Quarantine* action is not propagated to the downstream device in *Security Fabric > Automation*.
587758	Invalid CIDR format shows as valid by the Security Fabric threat feed.

Bug ID	Description
588262	IP address *Threat Feed* Fabric connector not working.

SSL VPN

Bug ID	Description
546280	Internal website (confluence.1wa.local) not loading all elements with SSL VPN web mode (it works fine internally).
559785	FortiMail login page with SSL VPN portal not displaying correctly.
561585	SSL VPN does not show correctly in the Windows Admin Center application.
571005	NextCloud through SSL VPN behaving strangely.
580182	The EOASIS website is not displayed properly using SSL VPN web mode.
586032	Unable to download report from an internal server via SSL VPN web mode connection.
588066	SSO for HTTPS fails when using "\" (backslash) with the domain\username format.
599668	In SSL VPN web mode, page keeps loading after user authenticates into internal application.
599671	In SSL VPN web mode, cannot display complete content on page, and cannot paste or type in the comments section.

Switch Controller

Bug ID	Description
592111	FortiSwitch shows offline CAPWAP response packet getting dropped/failed after upgrading from 6.2.2.

System

Bug ID	Description
527599	Internal prioritization of OSPF/BGP/BFD packets in conjunction with HPE feature to ensure these routing packets are handled in time. It affected all NP6 platforms.
527942	`diagnose firewall proute list` should not print `vwl_mbr_seq` if it is not generated by the VWL service rule.

Bug ID	Description
545449	IPinIP traffic over another IPinIP is dropped in NP6-Lite when offloading is enabled.
547712	HPE does not protect against DDoS attacks like flood on IKE and BGP destination ports.
548443	DHCP-enabled interfaces occasionally fail to perform discovery.
561234	FG-800D shows wrong HA, ALARM LED status.
573090	Making a change to a policy using inline editing is very slow with large table sizes.
576337	SNMP polling stopped when FortiManager API script executed onto FortiGate.
578531	The FortiCloud daemon (forticldd) resolves mgrctrl1.fortinet.com to the wrong IP address.
580883	DNS servers acquired via PPPoE in non-management VDOMs are used for DHCP DNS server option 6.
582498	Traffic can be offloaded to both NTurbo and NP6 when DoS policy is applied on ingress/egress interface in a policy with IPS.
582520	Enabling offloading drops fragmented packets.
586034	Enabling ECN dramatically decreases TCP throughput on FG-3400E.
586301	GUI cannot show default Fortinet logo for replacement messages.
588202	FortiGate returns an invalid configuration when FortiManager retrieves the configuration.
589079	QSFP interface goes down when the `get system interface transceiver` command is interrupted.
589234	Local system DNS setting instead of DNS setting acquired from upstream DHCP server was assigned to client under management VDOM.
592699	Console outputs `master change` information after entering `forticontroller` mode and `config-error-log`.
594577	Out of order packets for an offloaded multicast stream.
598357	Low throughput on subinterfaces VLAN because IP packets are marked with ECN = CE flag.
603194	NP multicast session remains after the kernel session is deleted.

User & Device

Bug ID	Description
547657	Guest portal RADIUS authentication failure due to FortiAuthenticator trying to resolve third-party websites as access points.
549662	RADIUS MSCHAP-v2 authentication fails against Windows NPS with non-ASCII characters in user password.
587519	fnbamd has high CPU usage and user is unable to authenticate.

Bug ID	Description
592241	Gmail POP3 authentication fails with certificate error since version 6.0.5.

VM

Bug ID	Description
577653	vMotion tasks cause connections to be dropped as sessions related to vMotion VMs do not appear on the destination VMX.
591563	Azure autoscale not syncing after upgrading to 6.2.2.
592611	HA not fully failing over when using OCI.

VoIP

Bug ID	Description
580588	SDP information fields are not being natted in multipart media encapsulation traffic.
582271	Add support for Cisco IP Phone keepalive packet.

WiFi Controller

Bug ID	Description
580169	Captive portal (disclaimer) redirect not working on Android phones.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
491701	FortiOS 6.0.9 is no longer vulnerable to the following CVE Reference: • CVE-2018-9195 Please read the section under *Upgrade Information > FortiGuard protocol and port number*.
565708	FortiOS 6.0.9 is no longer vulnerable to the following CVE Reference:

Bug ID	CVE references
	• CVE-2019-6696
569310	FortiOS 6.0.9 is no longer vulnerable to the following CVE Reference: • CVE-2019-15703

Known Issues

The following issues have been identified in version 6.0.9. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
581460	FG-30E AV TP mode cannot log and block oversize files.
590092	Cannot clear `scanunit vdom-stats` to reset the statistics on ATP widget.

Firewall

Bug ID	Description
508015	Editing a policy in the GUI changes the FSSO setting to disable.

FortiView

Bug ID	Description
527540	Cannot click the *Quarantine Host* option on a registered device.

Intrusion Prevention

Bug ID	Description
579018	IPS engine 5.030 signal 14 alarm clock crash at `nturbo_on_event`.

Log & Report

Bug ID	Description
592766	Log device defaults to empty and cannot be switched on in the GUI after enabling FortiAnalyzer Cloud.

Proxy

Bug ID	Description
584719	WAD reads `ftp over-limit multi-line` response incorrectly.

SSL VPN

Bug ID	Description
582265	RDP sessions terminate (disconnect) unexpectedly.

User & Device

Bug ID	Description
567831	Local FSSO poller is regularly missing logon events.

Built-In AV Engine

Resolved Engine Issues

Bug ID	Description
496255	Fixed some XML-based MS Office files recognized as ZIP files.
519759	Fixed `scanunit` crash when outbreak prevention is enabled.
530210	Added support for properly identifying and treating MSP file types.
530470	Fixed some HTML files that are identified as BAT files.
539279	Fixed after PDF is disarmed, PDF file is unreadable in Windows 10 Adobe Reader.
552133	Fixed content disarm wrongly detects MSP files.
564099	Fixed HTML/RedirME.INF!tr detection.
595481	Fixed AV engine false positive identifying XLSX file as an archive bomb.

Built-In IPS Engine

Resolved Engine Issues

Bug ID	Description
400997	Backport TLS 1.3 support for IPS engine 4.0.
466084	Added parameter default and multiple lines support; a new feature related to Mantis 466084 and the new SCADA/ICS NFR 571919.
478628	Fixed crash when copying to packet `mime_body` buffer. Fix crash when ZIP uncompressed size is bigger than `INT_MAX`.
513692, 594505	Fixed cross session tags with multiple engine processes.
519869	Fixed a specified service with default TCP protocol.
524362	Fixed IPS engine drops FIN-ACK packet for flow-based AV.
540344	In some cases when SNI verify failed, IPS engine crashed.
540902	Fixed reply to FIN+ACK retransmission with `seq=0&ack=0 pkt`.
545592	Fixed intermittent web access issue with SSL session ticket.
546787	In some rare cases, the RTP/RTSP/RTCP dissector resulted in a crash.
550227	Keep getting `attackid=0` in FortiGate IPS logs for P2P traffic.
552326	Port IPS tag database improvement patch for IPS 4.0.
554062	Fixed wait time too long in sniff mode.
554219	Always choose explicitly configured rules over implicit ones.
557379	Do not generate a random serial number for a resigned server certificate.
557944	Avoid padding oracles due to different handling of invalid record MAC and invalid paddings. Fixed incomplete HMAC validation and crashes. Fixed IPS engine crash when doing CBC HMAC validation.
561936	Fixed web rating overrides that do not work with an external proxy.
562832	Do not filter out application signatures based on applications detected in host session.
563177	Fixed incorrect SACK.
565955	Fixed IPS engine with high memory issue.
568328	Fixed botnet database loading crash on Windows and removed garbage strings from database.
568873	Fixed inconsistent local URL filtering for SSL sessions.

Bug ID	Description
569143	CIFS AV flow-based mode allows malware, which was blocked via HTTP. Change the value of `SMB2_OOO_LIMIT` to 4 MB.
570961	Apply URL filtering in packet error handler for certificate inspection as well.
574745	Create different sessions for the same session from a different policy.
579294	Support UTF-8 for flow web filter URLdatabase.
580113, 595060	Malware cannot be detected when both IPS and AV are enabled.
580113	Fixed HTTP decoder does not send file to flow-based AV.
584073	Fixed crash on HTTP2 control when getting content disposition.
586005	Fixed negative session expire time.
586544	Fixed IPS intelligent mode not working on random traffic.
587668	Fixed IPS engine signal 11 crash.
589653	Check null pointer before reference. Use `-Os` to compile for the FSOC2/FSOC3 platforms.
592618	Do not perform URL filter query if SNI is not yet verified.
593886	Use greased SSL extension to fill the gap in a session ticket extension.
594588	Fixed an IPS engine crash caused by session release.
594931	Check whether IPSA database is up-to-date before compile to avoid an unnecessary IPSA database compile.
596808	Fixed an IPS engine crash happening in SSL packet finish handler.
598036	Improved the way session ID cache cleans up. Reset SNI cache when it is around 90% full.

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.