FortiOS - Release Notes

Version 6.0.7

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

December 18, 2019
FortiOS 6.0.7 Release Notes
01-607-591521-20191218

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-11-13	Initial release.
2019-11-18	Changed 555805 to 582569 in *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2019-11-20	Removed 565708 from *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2019-12-18	Updated *Resolved Issues* and *Known Issues*.

Introduction

This document provides the following information for FortiOS 6.0.7 build 0302:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.7 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 6.0.7 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 6.0.7. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0302.

FG-30E-MG	is released on build 5411.
FG-1100E	is released on build 6519.
FG-1101E	is released on build 6519.
FG-VM64-AZURE	is released on build 5412.
FG-VM64-AZUREONDEMAND	is released on build 5412.
FG-VM64-RAXONDEMAND	is released on build 8529.

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
- FGR-30D
- FGR-35D
- FGR-60D
- FGR-90D
- FGT-200D

- FGT-200D-POE
- FGT-240D
- FGT-240D-POE
- FGT-280D-POE
- FGT-30D
- FGT-30D-POE
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E
- FGT-51E
- FGT-52E
- FGT-60D
- FGT-60D-POE
- FGT-70D
- FGT-70D-POE
- FGT-90D
- FGT-90D-POE
- FGT-94D-POE
- FGT-98D-POE
- FWF-30D
- FWF-30D-POE
- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E-2R
- FWF-50E
- FWF-51E
- FWF-60D
- FWF-60D-POE
- FWF-90D
- FWF-90D-POE
- FWF-92D

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 6.0.7 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 6.0.7.

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*.

Fortinet Security Fabric upgrade

FortiOS 6.0.7 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 6.0.7. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.7 and some running 5.6.x.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.0.7 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 6.0.7 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 6.0.7 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 6.0.7 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 6.0.7 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 11. 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 0282 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	• 6.00019
IPS Engine	• 4.00035
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 6.0.7. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
541023	Scan unit workers leave `urlfilter` API socket files behind in /tmp.
541577	FortiOS fails to upload files to FortiSandbox Cloud after upgrading the firmware from build 0804 to build 0828.

Application Control

Bug ID	Description
558380	Application control does not detect applications with `webproxy-forward-server`.

Data Leak Prevention

Bug ID	Description
540317	DLP cannot detect attached zip files when receiving emails via MAPI over HTTP.

DNS Filter

Bug ID	Description
567172	Enforcing safe search in 6.0.5 blocks access to Google domains.

Explicit Proxy

Bug ID	Description
504011	The FortiGate does not generate traffic logs for SOCKS proxy.
542230	Source affinity is held in the WAD dispatcher when the user is valid in the worker process.
543794	High CPU usage due to the WAD process.
552334	Websites do not work with SSL deep inspection due to the OCSP validation process.
557265	A browser redirect loop occurs after re-authentication when using `proxy-re-authentication-mode absolute`.
560076	SSL deep inspection is not performed on certain sites.

Bug ID	Description
561843	Application control unscans the traffic forwarded to the upstream proxy.
571034	Using a disclaimer causes incorrect redirection.
589811	The `urfilter` process does not start when adding a `dstaddr` category in a proxy policy with the deny action.

Firewall

Bug ID	Description
521913	Session timers do not update for VLAN traffic over VWP.
524599	Expired session TTL timers are not reset when traffic goes through if traffic is offloaded in a TP VDOM.
535468	The DCE/RPC `session-helper` expectation session is removed unexpectedly.
545056	The firewall should not be evaluated when an interface bandwidth widget is added to dashboard.
552329	NP6 sessions are dropped after any GUI changes.
554329	The schedule policy is not activated on time.
555287	VIPs should have a setting to control the SNAT behavior based on interfaces.
560674	Traffic to IP address configured in `internet-service-custom` is denied.
570468	The FortiGate randomly does not process some NAT64 packets.
571022	SNAT before encryption in policy-based VPNs for local traffic occurs after upgrading from 5.6.8 to 6.0.5.

FortiView

Bug ID	Description
539589	The `appFlag` is not updated after the cloud application database is updated.
541174	In *FortiView* > *Web Sites*, all categories are shown as *Unrated* (未分類) in Japanese.
553627	FortiView pages cannot load and present a "Failed to retrieve FortiView data" message.

GUI

Bug ID	Description
438298	When VDOMs are enabled, the interface faceplate should only show data for interfaces being managed by the admin.
479692	The GUI displays the error "Image file doesn't match platform" when the user uploads the correct image.

Bug ID	Description
487285	The *Monitor* > *FortiGuard Quota* > *View* category usage quota information displays "No matching entries found" for the local category.
512696	The *Unrated* category in *Web Rating Overrides* is translated incorrectly.
537307	"Failed to retrieve info" message appears for `ha-mgmt-interface` in *Network* > *Interfaces*.
537550	HTTPSD causes high CPU usage when accessing *Network* > *Interfaces*.
543637	Unable to filter policies by multiple IDs.
545074	Unable to log in into FortiOS with YubiKey. The CLI works as expected.
548076	FortiGateCloud cannot restore the configuration on the FortiGate.
548775	Cannot continue to configure the same column for different ports in *WiFi & Switch Controller* > *FortiSwitch Ports* unless the page is refreshed.
550098	An HTTP 400 error occurs when trying to activate FortiGate Cloud via the GUI.
552038	The routing monitor network filter does not filter subnets after upgrading.
552292	An HTTP 500 error occurs when trying to add a custom device into a custom device group.
553290	The tooltip for VLAN interfaces displays as "Failed to retrieve info".
564601	When using the GUI in USG mode, the license requirement to upload FortiGuard packages should be removed.
573579	Editing policies inline can result in previously selected policies being changed.
577112	When hovering over a Security Fabric name, a "Failed to retrieve info" message appears.

HA

Bug ID	Description
504156	Traffic is interrupted during an uninterruptible upgrade due to a down monitored port on the slave.
518964	The FortiGate slows down when adding or removing member from the address group via SSH.
519266	HA does not failover when the ping server goes down a second time.
538512	The `ha-direct` option does not affect the OCSP connection when the source IP is set.
539707	The ping server status is incorrect after failover in the output for `get sys ha status`.
543602	An unnecessary syncing process starts during upgrading when the upgrading takes longer.
545371	If the FortiGate sets two ping servers, there are dual masters.
546714	GARP packets are outputted even though the GARP setting is disabled.
547367	The slave cannot be synchronized from scratch in 6.0.4 with 500 VDOMs because duplicate global profiles are created.
548695	The FortiGate master does not send all system events.

Bug ID	Description
553231	Moving VDOMs between virtual clusters causes the cluster to go out of sync.
554187	The HA slave got and uncertified firmware signature after an image upgrade from the master.
555056	Enabling two-factor authentication for a virtual cluster in the GUI overwrites the sync from the slave to master.
555998	Load balanced (A-A) slave sessions do not forward traffic after the session is dirtied when installing a policy from FortiManager.
556057	`standalone-config-sync` shows members out of sync when there are four members.
574564	In an HA configuration with HA uninterruptible upgrade enabled, some signature database files may fail to synchronize when upgrading from previous versions.
581906	An HA slave sends out GARP packets 16-20 seconds after the HA monitored interface fails.

ICAP

Bug ID	Description
541423	After any configuration change is applied to the FortiGate, the Symantec ICAP server rejects connections due to many connections.

Intrusion Prevention

Bug ID	Description
545823	Creating and editing a DoS policy takes a long time. The GUI hangs up or displays an "Error 500: Internal Server Error".
556538	Enabling IPS on IPv4 policies impacts HTTPS traffic over the site-to-site VPN using PPoE for internal servers.

IPsec VPN

Bug ID	Description
509559	An invalid ESP packet is detected (replayed packet) when there is a high load on the IPsce tunnel.
515132	The ADVPN shortcut is continuously flapping.
522727	Dialup IPsec hardware acceleration drops.
534444	Unable to delete IPsec VPN tunnel phase1 interface configuration, even though there is no reference.
537450	Site-to-Site VPN policies (policy-based) with a DDNS destination fails to connect.
553759	ESP packets are sent to the wrong MAC after a routing change when IPsec SA is offloaded.
558693	FW-90D VPN becomes unresponsive after changing the VPN DDNS monitor settings.

Bug ID	Description
564237	SD-WAN interface bibandwidth is incorrect if it has recursive parents or if the parent has an estimated bandwidth set.
571209	Traffic over the VLAN subinterface is pushed through the IPsec policy based on the VPN interface.
582251	Peer ID validation does not work when IKEv2 EAP authentication is enabled.

Log & Report

Bug ID	Description
540157	Cannot view logs from the FortiGate when secondary the IP is used (only the secondary IP is allowed to go to the internet on upstream).
548038	An infinite loop seems to happen in `miglogd`.
552168	IPS archive pcap usage cannot be cleared after deleting the IPS log and actual pcap files.
558702	The main `miglogd` does not work until `sysctl killall miglogd`. Rebooting the device does not help.
560617	FortiGate logging is not stable; logs fail or do not stay in the queue.
562866	FortiOS 6.0.4/6.0.5 `reportd` crashes, possibly causing the FortiGate to go into conserve mode.
565216	`miglogd` memory increases and enters conserve mode.
566843	No log is generated when traffic is blocked by setting `tunnel-non-http` in `webproxy`.
568795	The specific traffic type is not logged in the FortiAnalyzer memory.

Proxy

Bug ID	Description
513470	WAD crashes on `wad_http_client_notify_scan_result.isra.XXX`.
529792	WAD process crash occurs with signal 11.
537183	Removing the default `ssl-exempt` setting causes the entries page to be empty.
540067	Wildcard addresses are removed from the SSL deep inspection exempt list after upgrading from 5.6.* to 6.0.4.
540368	When upgrading from 5.6.* to 6.0.*, the normal FQDNs get removed from the mixed FQDN group (normal and wildcard) from the SSL profile.
542189	An AV profile in proxy mode with `inspect-all` enabled causes a timeout when accessing some sites.
547426	WAD daemon crashes when upgrading to 6.2.0 build 0860.
549660	WAD crash occurs with signal 11.

Bug ID	Description
557259	A FortiGate using an AV profile in proxy mode with server comfort options enabled sends the same request to the server twice.
559166	With firmware 6.0.5, WAD CPU usage on all cores reaches 100% in about 30 seconds.
562610	The FortiGate generate a WAD crash `wad_mem_malloc`.
563154	Unable to open a webpage via explicit proxy when deep inspection and the web filter profile are enabled.
567796	WAD constantly crashes every few seconds.
572489	The SSL handshake sometimes fails due to the FortiGate replying "FIN" to the client.
574730	The wildcard URL filter stops working after upgrading.

Routing

Bug ID	Description
499330	OSPF MD5 authentication errors occur.
503686	`application pdmd` crash found.
536986	IPv6 routing fails to choose the lower priority route when the output interface is specified.
537054	The IPsec interface internet service router cannot work normally.
540682	SD-WAN sends traffic to interfaces with a volume ratio set to 0.
551492	BGP neighbors are lost on configuration changes (large configuration file).
552350	BFD peers are down and not seen (over BGP up).
557787	Although the routing table was changed in the IPv6 network, the offloaded communication stopped.
565661	SD-WAN interface bandwidth not honoring its parent's interface estimated bandwidth.
567497	The FortiGate sends PIM register messages to RP for group 64.0.0.0 about non-existent sources.
573789	OSPF with virtual clustering is not learning routes.
578623	The memory gradually increases with a full BGP table.

SSL VPN

Bug ID	Description
481038	Web application does not load through the SSL VPN portal.
489110	SSL VPN web mode fails to access the Angular 5 application.

Bug ID	Description
491733	When the SSL VPN receives multiple https post request under web filter, there is a loop of `read_request_data_f` even when the client stops, causing the SSL VPN process to use 99% of the CPU.
496584	Wrong password attempts cause excessive bind requests against LDAP and lock out accounts.
509333	Nextcloud does not open in SSL VPN web mode.
513572	FortiGate does not send framed IP address attribute in RADIUS accounting packet.
513655	SMB/CIFS bookmark in the SSL VPN portal does not work with the `username` variable; the return error is “Invalid HTTP request”.
515889	SSL VPN web mode has trouble loading the internal web application.
527476	Web mode update fails for SharePoint pages using MS NLB.
530509	"Invalid HTTP Request" when an SMB via SSL VPN bookmark is executed with MS Server 2016, but does work with MS server 2008R2.
534728	Unable to get the dropdown menu from the internal server via SSL VPN web mode connection.
535739	SSL VPN bookmarks fail with JavaScript error.
539207	Unable to get to http://spiceworks.int.efwnow.com:9750/tickets/v2#open_tickets via the SSL VPN bookmark.
539948	Unable to load webpage in SSL VPN web mode.
540328	When trying to access an internal server with SSL VPN web mode, the browser displays an "ERR_EMPTY_RESPONSE" message.
542480	The internal server script gets stuck loading when a page is accessed over the SSL VPN web portal.
542706	When authenticating a user with local entry (local or remote authentication), there is no information available about the groups in which the user belongs to, so user-based policies are applied.
545177	Web mode fails on SharePoint pages.
546187	SSL VPN login authentication times out if the primary RADIUS server is unavailable.
546748	Cannot log in to an internal server through SSL VPN web mode.
547069	Customer's application is not displayed correctly in SSL VPN web mode.
551535	HTTP 302 redirection is not parsed by the SSL VPN proxy (web mode/bookmark).
552018	JavaScript errors occur when accessing internal websites in web mode.
554821	Display problems occur with web mode access in FortiOS 6.2.0 and 6.0.4.
555983	The internal web potal replies with "HTTP 404 Not Found" when accessed via the SSL VPN web portal bookmark.
556657	Internal websites not working through SSL VPN web mode.
559790	SSL VPN web mode is not proxying internal websites correctly.
559932	Customer unable to load website through SSL VPN web mode.

Bug ID	Description
563147	The connection to internal portal freezes when using an SSL VPN web bookmark.
567182	Videos on internal website do not display in web mode.
567987	RDP disconnects in web mode when copying long text from remote to local.
569030	SSL VPN tunnel mode can only add split tunneling to a user policy with groups and users in different SSL VPN policies.
573527	SSL web portal CSP v3 compatibility issue.
575248	Synology DSM log in page is not displayed when accessed via an SSL VPN bookmark or connection tool.
575259	SSL VPN connection is being dropped intermittently.
578581	Web mode portal freezes when opening some websites using JavaScript.

Switch Controller

Bug ID	Description
545331	FortiSwitch object cannot be created through FortiManager, but can be created in the FortiOS CLI.
549770	FortiSwitch `export-to` commands do not sync, causing an HA sync problem.
555366	FortiGate is not pushing the `trunk/lldp-profile` configuration to FortiSwitch when there is a space in the entry name.
586299	Adding a factory reset device to HA fails with the switch-controller.qos settings in root.

System

Bug ID	Description
470875	OID seems to COUNTER32 instead of GAUGE32.
484749	TCP traffic with the ECN bit cannot pass through the IP tunnel with NP6 offload enabled.
493843	SNMPD debug messages reveal source code function names.
502387	X.509 certificate support required for the FGFM protocol.
511529	`vdom-property` limits error occurs after upgrading from 5.4.6 to 5.6.3.
514676	On a multi-processor platform, fragment evictor can run on multiple CPUs, which will result in multiple CPUs competing for locks.
515735	DHCP proxy functionality issue over IPsec with IKEv1 and IKEv2.
518655	IPv6 does not respond to neighbor solicitation requests.
527124	CRL download fails with the error message "Operation now in progress".
533214	After executing a shutdown, FG-90E keeps responding to ICMP requests.
535055	When adding more than seven VPN tunnels to the SD-WAN, PPoE default routes disappear.

Bug ID	Description
537571	IPS/AV is not forwarding return traffic back to clients.
537989	Kernel static route is randomly lost.
539916	TCP SYN+ACK is not forwarded under a specific condition.
539970	Kernel panic on HA pair of FG-301Es.
541243	DHCP option doesnot include all NTP servers.
541527	Changing the order of VDOMs in system admin when connected with TACACS+ wildcard admin is not propagated to other blades.
543054	Setting `alias` or changing allowed access to the aggregate link will move the from state down to up for few seconds.
544570	Master unit does not send the SNMP trap for all SNMP servers when the cable is plugged out from the LAG-configured interface.
544828	FG-301E consumes high memory even when there is no traffic.
545717	Huawei E173u-2 USB modem not working on FG-60E.
546746	Cannot lease DHCP address over IPsec for dialup FortiClient users.
548553	VDOM restore has configuration loss when interfaces have subnet overlap.
550433	*/tmp/fcp_rt_dump* file lost some IPsec VPN router information after modifying the IPsec VPN static router setting.
553262	TCP connections through IPsec (bound to loopback) do not work when IPS offload is enabled to NTurbo.
553609	In FortiOS 6.2.0 FortiExplorer management via a USB connection, it takes a very long for the device to show up.
554099	Cannot poll SNMP v3 statistics for BGP when `ha-direct` is enabled under `snmp user`.
555992	Changes to per-IP shaper settings are not reflected on offloaded sessions.
557798	High memory utilization caused by `authd` and `wad` process.
560411	FG-3980E unresponsive with millions of sessions in TIME_WAIT.
560686	4x10G port does not work on FG-3700D.
561097	SD-WAN rule corrupted upon rebooting after ISDB update.
561409	Current slave interface of redundant interface does not change according to member settings.
561929	REST API `cmdb/router/aspath-list` is not inserting new values.
563497	The `trust-ip-x` feature for interfaces does not work.
565291	SD-WAN rule does not work with nested firewall address group when it is selected as a source or destination.
565631	DHCP relay sessions are removed from the session table after applying any configuration change.

Bug ID	Description
567487	CPU usage goes to 100% when modifying members of an `addrgrp` object.
570575	PoE ports no longer deliver PoE power.
570759	RX/TX counters for VLAN interfaces based on the LACP interface are 0.
574110	When adding an admin down interface as a member of an aggregate interface, it shows as up and processes traffic.
577047	FortiGate takes a long time to reboot when it has a very large amount of firewall addresses used in a large amount of policies.
578259	VLANs over the LAG interface show no TX/RX statistics.
578746	FortiGate does not accept country code created in FortiManager and causes address install fails.
577955	LTE modem drops with crash log when IPsec tunnel is brought up.

Upgrade

Bug ID	Description
558995	L2 WCCP stops working after upgrading to FortiOS 6.0.3 or later.
562444	The firewall policy with `internet-service` enabled was lost after upgrading from FortiOS 6.0.5.

User & Device

Bug ID	Description
516403	FSSO established sessions are not re-evaluated when an user is removed from an Active Directory group.
518129	FSSO failover is not graceful.
538218	Mobile token authentication fails in a virtual cluster on the physical slave.
538407	FortiOS does not allow a source IP to be set for mobile token activation
538666	FortiToken assignment on a virtual cluster VDOM master on a physical slave causes configuration mismatch and physical master overwrites.
546600	Cannot set certificate under `config certificate local`.
548460	`set device-identification disable` reverts to default after restoring the VDOM.
550512	Wireless roaming causing the undesirable removal of RSSO sessions.
558332	CoA from FortiAuthenticator is not working for a wired interface-based captive portal.
560360	Both authenticated and unauthenticated sessions are cleared when authentication times out.
561289	User-based Kerberos authentication is not working in new VDOMs.

Bug ID	Description
562185	Disclaimer redirection to IP instead of FQDN, resulting in an SSL certificate warning.
572271	MAC host updates cause the sessions to be marked as dirty.

VM

Bug ID	Description
505520	VMX does not sync the contract information from SVM.
541531	VMX 6.0.4 Service Manager is not automatically updated with the NSX dynamic security groups.
545533	The default MTU of 65521 results in packet drops.
559051	Azure waagent process is consuming high memory.
567137	VM in Oracle cloud has 100% CPU usage in the system space.
579948	New FGCP master does not update AWS route tables to reference the correct ENI.

VoIP

Bug ID	Description
570430	SIP ALG generated a VoIP session with the wrong direction.

WAN Optimization

Bug ID	Description
542047	Cannot create new directory on the FTP server with `mkdir` from an FTP client through a WAN optimization tunnel.
564290	FortiOS cannot collaborate web cache with FortiProxy successfully.

Web Filter

Bug ID	Description
551956	Proxy web filtering blocks innocent sites due to `urlsource="FortiSandBox Block"`.
565952	Proxy-based web filter breaks the WCCP traffic.

WiFi Controller

Bug ID	Description
529931	Wireless MAC address filtering stopps working after upgrading from 5.6.6 to 6.0.3.
556022	WiFi certificate settings become empty and eap_proxy stops after deleting the CA bundle package and rebooting the FortiGate.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
395544	FortiOS 6.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2017-17544
532730	FortiOS 6.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2019-6693
548154	FortiOS 6.0.7 is no longer vulnerable to the following CVE References: • 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
567521	FortiOS 6.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2019-6697
578626	FortiOS 6.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2019-15705
582569	FortiOS 6.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2019-5593

Known Issues

The following issues have been identified in version 6.0.7. 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.

FortiView

Bug ID	Description
556178	*Sources* historical view sometimes cannot retrieve data from FortiCloud.

GUI

Bug ID	Description
546580	Should not be allowed to unset user/group on an SSL VPN policy when inline editing the source column in the policy list.
556397	IP pools in the SSL VPN settings are overwritten when the SSL VPN settings are modified in the GUI.
559866	When sending a CSF proxied request, segfault happens (httpsd crashes) if FortiExplorer accesses the root FortiGate by the management tunnel.
566230	FortiOS 6.0.4 GUI access is very slow when creating, editing, or adding policies.

HA

Bug ID	Description
523582	`hamgmt` gateway IP gets synced from master to slave after restoring configurations.
530215	`application hasync` returns "*** signal 11 (Segmentation fault) received ***".

IPsec VPN

Bug ID	Description
542905	IKE route overlap should be allowed across two distinct dialup `phase1`s.

Bug ID	Description
550333	When an ADVPN spoke has one interface that connects to two hubs, the shortcut created on the receiver side could match to the wrong `phase1`.
575477	IKED memory leak occurs.

Log & Report

Bug ID	Description
493886	`reportd` is sometimes stuck at 99% CPU usage.
586038	VPN tunnel durations are too long in the local reports for FortiOS 6.0.6.
592366	Cannot display *Forward Traffic* logs when filtering by source IP or policy ID.
592766	Log device defaults to empty and cannot be switched on in the GUI after enabling FortiAnalyzer Cloud on FG-101F.

Proxy

Bug ID	Description
566859	In WAD conserve mode in 5.6.8, the `max_blocks` value is high on some workers.

Routing

Bug ID	Description
581488	The BGP confederation router sends an incorrect AS to neighbor group routers.

Security Fabric

Bug ID	Description
583107	The *Access Layer Quarantine* action is not propagated to the downstream device in *Security Fabric > Automation*.

SSL VPN

Bug ID	Description
561585	SSL VPN does not show correctly in the Windows Admin Center application.
586032	Unable to download report from an internal server via SSL VPN web mode connection.

System

Bug ID	Description
527942	`diagnose firewall proute list` should not print `vwl_mbr_seq` if it is not generated by the VWL service rule.
548443	DHCP-enabled interfaces occasionally fail to perform discovery.
550701	WAD daemon signal 11 causes `cmdbsvr` deadlock.
573090	Making a change to a policy using inline editing is very slow with large table sizes.
578531	The FortiCloud deamon 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.
589079	QSFP interface goes down when the `get system interface transceiver` command is interrupted.

User & Device

Bug ID	Description
549662	RADIUS MSCHAPv2 authentication fails against the Windows NPS when the user password contains non-ASCII characters.
561610	`src-vis` process memory leak occurs.
567831	The local FSSO poller is regularly missing logon events.
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.

VoIP

Bug ID	Description
580588	SDP information fields are not being NAT'd in multi-part media encapsulation traffic.
582271	Add support for Cisco IP phone keepalive packet.

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.