FortiOS - Release Notes

Version 6.0.4

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET COOKBOOK
https://cookbook.fortinet.com

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdocs@fortinet.com

January 10, 2019
FortiOS 6.0.4 Release Notes
01-604-527518-20190110

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-01-10	Initial release.

Introduction

This document provides the following information for FortiOS 6.0.4 build 0231:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.4 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-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-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-5001D, FG-3960E, FG-3980E, 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-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-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCPONDEMAND
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 6.0.4 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 6.0.4. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0231.

FG-60E-DSL	is released on build 5168.
FG-60E-DSLJ	is released on build 5168.
FWF-60E-DSL	is released on build 5168.
FWF-60E-DSLJ	is released on build 5168.

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 6.0.4 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 5.6.6 or higher, or 6.0.2 or higher.

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

- FortiAnalyzer 6.0.0
- FortiClient 6.0.0
- FortiClient EMS 6.0.0
- 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 6.0.4. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.4 and some running 5.6.x.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.0.4 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 6.0.4 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 6.0.4 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 6.0.4 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 6.0.4 product integration and support information:

Web Browsers	• Microsoft Edge 41 • 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.
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)	• 3.6.4 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 0272 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8

FortiExtender	• 3.2.1
AV Engine	• 6.00019
IPS Engine	• 4.00029
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
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 61 Google Chrome version 68
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 61 Google Chrome version 68
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
OS X El Capitan 10.11.1	Apple Safari version 11 Mozilla Firefox version 61 Google Chrome version 68
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 6.0.4. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
516072	In flow mode, `scanunit` API does not allow IPS to submit scan job for URL with no filename.
519759	Process `scanunit` crashes.
522343	`scanunitd` having constant different kind of crash.

Endpoint Control

Bug ID	Description
495132	Automation stitch IOC for Access Layer Quarantine works incompletely.

Explicit Proxy

Bug ID	Description
521344	Explicit FTP proxy doesn't work with secondary IP address.
521899	When proxy `srvc` is set to protocol CONNECT and client tries to connect to HTTPS page, client gets message: Access Denied.
523974	Cannot access some web sites with deep inspection enabled.

Firewall

Bug ID	Description
390422	When a firewall address group is used in firewall policy, a wildcard FQDN address should not be allowed to be added into the firewall address group as a member.
503904	Creating a new address group gives error: `Associated Interface conflict detected!.`
504057	Service Object Limitation of 4096 needs to be increased.
511261	RSH connection disconnects when we have multiple commands executed via script and we can see the message `no session matched`.
514187	VIP ping healthchecks fail with high number of realservers.

FortiView

Bug ID	Description
256264	Realtime session list cannot show IPv6 session and related issues.
453610	*Fortiview >Policies(or Sources) >Now* shows nothing when filtered by physical interface at PPPoE mode.
460016	In *Fortiview* > *Threats*, drill down one level, click *Return* and the graph is cleared.
461811	In Cloud Applications widget bubble view, the tooltip cannot display Application.
488886	*FortiView* > *Sources* is unable to sort information accurately when filtering by policy ID number.
495070	In *FortiView* > *Cloud Applications* > *Applications*, GUI keeps loading and without any response.
527700	FortiView pages cannot be loaded by latest Chrome version 71.0.3578.80.

GUI

Bug ID	Description
437117	In Single Sign-on, multiple FSSO polling servers with the same AD (LDAP) server cannot select the same user or group.
456289	GUI to support two-level device classification schema.
491919	GUI - Routing Monitor page does not load with large number of routes inserted in the routing table.
497427	V3.3.0_533151 remote access stuck loading main dashboard page and login with Fortimanager_ Access user.
512806	Slowness in loading the Addresses page.
515022	FortiGate and FSA has right connectivity, but Test Connectivity on GUI interface is showing `Unreachable or not Authorized`.
515983	Firefox cannot list user *TACACS+ Servers*. Chrome is OK.
516027	In GUI IPsec monitor page, the column *username* should be *peerID*.
516295	`Error connecting to FortiCloud` message while trying to access FortiCloud Reports in GUI.
518024	Guest admin logging in gets GUI Error 500: Internal Server Error.
518131	Cannot add static route with the same gateway IP and interface from WebGUI.
518970	Suggestion to improve SD-WAN SLA creation page's invalid-entry handling.
522576	GUI always loading VPN interface when there is over 5k VPN tunnel interfaces.
526573	GUI Virtual IP misses SSL-VPN interface.

HA

Bug ID	Description
445214	Slave in AP cluster memory/CPU spike as a result of DHCP/HA sync issue.
509557	Duplicate MAC on mgmt2 ports.
510660	Upgrade to build 3574 fails for HA cluster.
511522	HA uninterruptible upgrade from 9790 to 3558 fails.
515401	SLBC-Dual mode: Slave chassis blade sending traffic logs.
516779	Confsync cannot work with three members when encryption is enabled.
517537	Slave out-of-sync. Unable to log into slave unit.
518621	`ha-mgmt-interface` IPv6 GW is not registered when `ha-mgmt-interface` IPv4 GW is **not** set.
518651	TCP Session lost when only one unit in HA cluster kicked un-interruptive upgrade.
519653	Increase FGSP session sync from 200 VDOMs to 500 VDOMs.
525182	WLAN guest user in VDOM makes the cluster out of sync.

Intrusion Prevention

Bug ID	Description
469608	ICMP packets dropped during FortiGate update.
476219	Delay for BFD in IPinIP traffic hitting policy with IPS while IPsec calculates new key.
501986	DOS policy configured with action proxy for `tcp_syn_flood` doesn't work properly.
516128	Victim is quarantined after IPS attack.

IPsec VPN

Bug ID	Description
515375	VPN goes down randomly, also affects remote sites dialup.
520151	When two certificates are configured on p1, both aren't offered or the wrong one is offered.

Log & Report

Bug ID	Description
503897	FortiGate-501E units generating logs only for five minutes after rebooting the unit, Then do not generate logs anymore.
516033	The traffic log for WANOPT data traffic in the server-side FortiGate should show policy type as *proxy-policy*, not *policy*.

Bug ID	Description
518402	`miglogd` crash and no logs are generated.
522447	FortiGate logging is not stable and stops working.
522512	When a service group contains more than 128 services, the existing logic cannot catch it and causes buffer overflow.
519969	EXE log filter category `utm-anomaly/utm-voip` does not work.

Proxy

Bug ID	Description
477289	Proxy is unexpectedly sending FIN packet (FTP over HTTP traffic).
509994	Web site denied due to certificate error (revoked) only in Proxy_policy and deep inspection profile.
512434	Need to do changes in default replacement message of `Invalid certificate Message`.
513270	Certificate error with SSL deep inspection.
514426	Explicit proxy cannot catch Microsoft Outlook after FFDB update.
516414	Traffic over 1GB through SCP gets terminated when SSH inspection is enabled in `ssl-ssh-profile`.
516934	In transparent proxy policy with cookie authentication mode, NTLM authentication doesn't work and LDAP authentication using wrong username/password will cause WAD to crash.
519021	Cannot access internal CRM application server with antivirus enabled.
521051	HTTP WebSocket 101 switching protocol requests mismatch in 6.0.3.
521648	WAD crashes and `fnbamd` process takes 100% of CPU. Kerberos and NTLM authentication do not work
526322	WAD crashes when processing transparent proxy traffic after upgrade to 6.0.3.
526555	WAD segmentation signal 11 in 6.0.3.

REST API

Bug ID	Description
467747	REST API user cannot create API user via autoscript upload and cannot set API password via CLI.

Routing

Bug ID	Description
441506	BGP Aggregate address results in blackhole for incoming traffic.
449010	WAN LLB session log `srcip` and `dstip` are mixed up intermittently.

Bug ID	Description
476805	FortiGate delays to send keepalive which causes neighbor's hold down timer to expire and reset the BGP neighborship
485408	Merge vwl_valeo project - no option for `proute` based on only dynamic routes.
500432	IGMP multicast joins taking very long time and uses high NSM CPU utilization.
515683	FortiGate generates fragmented OSPFv3 DBD packets.
518677	Log message `MOB-L2-UNTRUST:311 not found in the list!` seen on VDOM with IPv6 router advertisement enabled.
518929	SNMP, OSPF MIB ospfIfState value when designated router is not correct.
518943	RIPv2 with MD5 authentication key ID incompatible with other vendors.
520907, 520945	Zebos doesn't start up correctly on models using Linux 2.4 kernel.
522258	Some missing fields in `proute` list.

Security Fabric

Bug ID	Description
515970	Fabric settings/widget and FortiMail icons are yellow even when they are connected.

SSL-VPN

Bug ID	Description
508101	HTTPS bookmark to internal website produces error after the initial successful login.
511002	SSL-VPN web mode login fails when entering valid OTP manually.
511107	For RADIUS with 2FA and password renewal enabled, password change fails due to unexpected state AVP + GUI bug.
511415	SSL-VPN web mode RDP connection disconnects when pasting text from local to remote RDP server.
515889	SSL-VPN web mode has trouble loading internal web application.
519068	WAD informer process crashes in tunnel mode SSL-VPN user login.
519372	SSL-VPN web mode RDP doesn't work.
519987	HTTP bookmark error `SyntaxError: Expected ')'` after accessing internal server.
520361	SSL-VPN portal not loading predefined bookmarks.
521459	HSTS header missing again under SSL-VPN.

Switch Controller

Bug ID	Description
522457	After a physical port of FortiLink LAG has link down/up, `fortilinkd` packet cannot be sent from FortiGate to FortiSwitch.

System

Bug ID	Description
502651	Inconsistent behavior with 1G copper transceivers on 3960E.
503318	Accessing FDS via proxy server without DNS resolution.
505468	Incorrect SNMP answer for `get-next`.
505522	Intermittent failure of DHCP address assignment.
505873	`ftm2` daemon cannot detect change of `ssl-static-key-ciphers` and need to restart daemon.
507518	Partial configuration loss after root VDOM restore.
508285	After restoring a config for VDOM, the VDOM cannot be deleted unless OS is rebooted.
510737	Users are not able to pull DHCP addresses from FGT.
511851	Unable to set EMAC VLANs on different VDOMs to the same VLAN ID.
512930	WAD crash with signal 11.
513156	Packet loss on startup when interfaces are in bypass mode (2500E).
513339	Finisar FCLF8521p2BTL (FG-TRAN-GC) and (FS-TRAN-GC) FCLF8522P2BTL transceivers not detected by FortiOS.
513663	FG-3200D running FOS 5.6.5 – WAD crashing frequently.
516105	Daylight Saving Time no longer used in Azerbaijan.
516783	DSA and RSA fingerprints are identical.
524422	Support FortiGateRugged-30D model containing the new CPU.

Upgrade

Bug ID	Description
510447	FWF-30D keeps rebooting after upgrade to 6.0.2.

User & Device

Bug ID	Description
463849	FAC remote LDAP user authentication via RADIUS fails on invalid token if password change and 2FA are both required.
491118	Kerberos users unable to access internet.
510581	Backup password for LDAP admin does not work when interface is down.
511776	Once user has assigned token other tokens not listed in pull down menu.
515226	FortiGate keeps sending accounting packet to RADIUS server for user that is no longer authenticated.
519826	`fnbamd` crashes and LDAP authentication stops working after upgrade.

VM

Bug ID	Description
488964	Service Manger warns that internal and external interfaces are down.
498653	FortiOSVM stops passing traffic after failover.
509672	"netx request error:60…" was reported when running some "exec nsx service" and "exec nsx group" commands on SVM.
512713	Connectivity loss between FGT-SVM and FGT-VMX causes license to became invalid after one hour.
515624	FortiGate VM cannot use the maximum memory allowance as per the license.
524852	Possible cross-origin error when attempting to read state from window.opener for GCP marketplace.

VoIP

Bug ID	Description
516927	No audio when call is generated from the outside in a FGT30E SIP-ALG when local devices apps register against remote SIP server.

Web Filter

Bug ID	Description
486171	The "Web Rating Overrides" doesn't work with flow-mode.
518933	Certificate inspection (CN base) web category filter doesn't work.
523804	Enabling safe search on DNS causes any site with *google* in the domain to redirect to *forcesafesearch.google.com*.

WiFi Controller

Bug ID	Description
478594	`wpad_ac` uses high CPU.
503106	Remote site client connected to the FAP14C ethernet port is randomly not able to reach the LAN client connected to the FortiGate.
512606	FortiWiFi not working with FortiPresence Pro.
519321	FWF-50E kernel panic due to a WiFi driver issue.
520521	`hostapd` crashes and causes a wireless outage.
522762	Frequent `hostapd` crash.

Known Issues

The following issues have been identified in version 6.0.4. 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.
488369	DSCP/ToS is not implemented in shaping-policy yet.

FortiView

Bug ID	Description
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
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.
482045	FortiView – no data shown on *Traffic from WAN*.
521497	The FortiView All Sessions real time view is missing right-click menu to end `session/ban ip`.
525702	FortiView does not support auto update in real-time view and shows unscanned application.
526956	FortiView widgets get deleted on upgrading to B222.
527540	In many FortiView pages, the *Quarantine Host* option is not clickable on a registered device.
527708	Policy ID hyper link in policy view is missing.
527775	FortiView logs entries do not refresh on log drill down page.
527952	*FortiView* > *WiFi Clients* > *drill down* > *Sessions* gets nothing at final drill down if device identification is disabled.
528483	*FortiView* > *Destination* page filter *destination owner* cannot filter out correct destination in real time view.
528684	*FortiView* > *Bubble Chart* cannot drill down on Firefox 63 with ReferenceError: "event is not defined".
528744	*FortiView* > *Traffic Shaping* displays data with error message if switched from other pages in custom period.
528767	In *FortiView* > *multiple charts*, *Previous Time Periods* in custom period is missing.

Bug ID	Description
529000	Threat view does not show entries if signature attack direction is incoming and the source is FortiAnalyzer.
529001	In *FortiView* > *Cloud Applications*, there are entries without cloud action details.
529313	*FortiView* > *Web Sites* > *Web Categories* drill down displays all entries in *Policies* tab.
529355	All tabs in *FortiView* > *System Events* show no entry when the source is FortiCloud.
529558	*System Events* widget shows *No matching entries found* when drilling down HA event.

GUI

Bug ID	Description
439185	AV quarantine cannot be viewed and downloaded from detail panel when source is FortiAnalyzer.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
451776	Admin GUI has limit of 10 characters for OTP.
508015	Edit Policy from GUI changes `fsso` setting to disabled.
513451	Archived data filed in logs shows incorrect data.
516415	*Edit Disclaimer Message* button is missing on *Proxy Policy* page.

HA

Bug ID	Description
451470	Unexpected performance reduction in case of Inter-Chassis HA fail-back with enabling HA override.
479987	FG MGMT1 does not authenticate Admin RADIUS users through primary unit (secondary unit works).
529274	Factory reset box faild to sync with master in multi-VDOM upgraded from 6.0.3.

Intrusion Prevention

Bug ID	Description
445113	IPS engine 3.428 on FortiGate sometimes cannot detect Psiphon packets that iscan can detect.

IPsec VPN

Bug ID	Description
469798	The interface shaping with egress shaping profile doesn't work for offloaded traffic.
481201	The OCVPN feature is delayed about one day after registering on FortiCare.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create web filter logs.
528786	In Log viewer, forward traffic filter Result Accept(all)/Deny(all) does not work.

SSL-VPN

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

Switch Controller

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.

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.
364280	User cannot use `ssh-dss` algorithm to login to FortiGate via SSH.
385860	FG-3815D does not support 1GE SFP transceivers.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
468684	EHP drop improvement for units using `NP_SERVICE_MODULE`.
472843	When FortiManager is set for `DM = set verify-install-disable`, FortiGate does not always save script changes.
474132	FG-51E hang under stress test since build 0050.
494042	If we create VLAN in VDOM A, then we cannot create ZONE name with the same VLAN name in VDOM B.
513339	Finisar FCLF8521p2BTL (FG-TRAN-GC) and (FS-TRAN-GC) FCLF8522P2BTL transceivers not detected by FortiOS.

Upgrade

Bug ID	Description
470575	After upgrading from 5.6.3, `g-sniffer-profile` and `sniffer-profile` exist for IPS and web filter.
473075	When upgrading, multicast policies are lost when there is a zone member as interface.
481408	When upgrading from 5.6.3 to 6.0.0, the IPv6 policy is lost if there is SD-WAN member as interface.
494217	Peer user SSL VPN personal bookmarks do not show when upgrade to 6.0.1. **Workaround**: Use CLI to rename the user bookmark to the new name.

Web Filter

Bug ID	Description
480003	FortiGuard category does not work in NGFW mode policy.

WiFi Controller

Bug ID	Description
516067	CAPWAP traffic from non-VLAN SSID is blocked when `dtls-policy=ipsec-vpn` and NP6 offload are enabled.

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.