FortiOS - Release Notes

Version 6.0.3

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

November 1, 2018
FortiOS 6.0.3 Release Notes
01-603-515361-20181101

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Supported models 5
Special branch supported models 6
Special Notices **7**
WAN optimization and web caching functions 7
FortiGuard Security Rating Service 7
Built-in certificate 8
FortiGate and FortiWiFi-92D hardware limitation 9
FG-900D and FG-1000D 9
FortiClient (Mac OS X) SSL VPN requirements 9
FortiClient profile changes 10
Use of dedicated management interfaces (mgmt1 and mgmt2) 10
Using FortiAnalyzer units running older versions 10
Upgrade Information **11**
Fortinet Security Fabric upgrade 11
Minimum version of TLS services automatically changed 11
Downgrading to previous firmware versions 12
Amazon AWS enhanced networking compatibility issue 12
FortiGate VM firmware 13
Firmware image checksums 13
FortiGuard update-server-location setting 14
Product Integration and Support **15**
Language support 16
SSL VPN support 17
SSL VPN standalone client 17
SSL VPN web mode 17
SSL VPN host compatibility list 18
Resolved Issues **20**
Known Issues **30**
Limitations **34**
Citrix XenServer limitations 34
Open source XenServer limitations 34

Change Log

Date	Change Description
2018-10-09	Initial release.
2018-10-10	Updated 511394 in *Resolved Issues*.
2018-10-15	Updated *Product Integration and Support > SSL VPN standalone client* to specify 32-bit & 64-bit for Linux Ubuntu. Added *Using FortiAnalyzer units running older versions* to *Special Notices*. Deleted unnecessary warning in *Upgrade Information*. Deleted 474612, 470589, 493839, 466048, 482497, 494603 in *Known Issues*.
2018-10-25	Added 496642 to *Resolved Issues*.
2018-10-29	Added *Introduction > Special branch supported models*.
2018-11-01	Deleted 440411 in *Known Issues*. Added 488369 to *Known Issues*.

Introduction

This document provides the following information for FortiOS 6.0.3 build 0200:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.3 supports the following models.

FortiGate	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-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 6.0.3 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 6.0.3. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0200.

FG-30D	is released on build 5117.
FG-30D-POE	is released on build 5117.
FWF-30D	is released on build 5117.
FWF-30D-POE	is released on build 5117.

Special Notices

- WAN optimization and web caching functions
- FortiGuard Security Rating Service
- Built-in certificate
- FortiGate and FortiWiFi-92D hardware limitation
- FG-900D and FG-1000D
- FortiClient (Mac OS X) SSL VPN requirements
- FortiClient profile changes
- Use of dedicated management interfaces (mgmt1 and mgmt2)

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 6.0.3 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 6.0.3 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 6.0.3. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.3 and some running 5.6.x.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.0.3 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 6.0.3 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 6.0.3 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 6.0.3 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 6.0.3 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 . 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 0271 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	• 6.00012
IPS Engine	• 4.00025
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	✔

Language	GUI
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

Operating System	Web Browser
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	✔	✔

Product	Antivirus	Firewall
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 6.0.3. For inquires about a particular bug, please contact Customer Service & Support.

Anti-Spam

Bug ID	Description
500789	FortiGuard spam submission hyperlink does not contain any link to to the FortiGuard submission page.

Antivirus

Bug ID	Description
445312	`tcp-timewait-timer` does not have any effect when WAD is running.
459986	Repeated scanunit signal 11 crash scan_for_base64_objects.
502138	AV full scan mode causes traffic to fail.
505249	Proxy AV profile blocks Dell Command Update.
505393	Quad File Dropped Reason `forticloud-daily-quota-exceeded`.

Application Control

Bug ID	Description
498396	Upgrade from 5.2.13 to 5.4.9 is affected by application list global limit.

Data Leak Prevention

Bug ID	Description
454103	Certain PDF files are blocked when DLP filter is set to block `.bat` file.
496255	Some XML-based MS Office files are recognized as ZIP file.
506750	Customer wants to block `.csv` file extension when attaching a file on web-based gmail.

Endpoint Control

Bug ID	Description
479672	FortiTelemetry not blocking VIP.
500027	Can't block FortiClient that's not compliant.

Explicit Proxy

Bug ID	Description
496294	SNMP value returned OID of `fgExplicitProxyMemUsage` and `fgExplicitProxyUpTime` is always 0.
502392	Explicit web proxy does not learn session TTL correctly.
503478	Presence of `X-XSS-Protection` header causes response to be not cacheable.
506654	High memory usage on WAD.
508818	Agentless NTLM proxy authentication incorrectly returns `403 Authorization Failed` to empty credential login attempt.
509876	Web proxy internet service as `dst` address cannot work for some IP address range overlap cases.
512268	FortiView is not populated by `xff-learned` original client IP address.
512294	WAD should not keep buffer data if the server's response broke the HTTP protocol.

Firewall

Bug ID	Description
504699	`nat-source-vip` enabled shouldn't affect SNAT in normal policy.
506430	Traffic shaper bandwidth cannot exceed guaranteed bandwidth if max bandwidth is not configured.
508844	FortiGate needs to support NAT64 fragmentation inbound DF-set feature.
509777	Default custom service will block traffic.

FortiView

Bug ID	Description
507441	Unable to show information from GUI in *Fortiview* > *Sources*.

GUI

Bug ID	Description
297832	Administrator with read-write permission on *Firewall Configuration* is not able to read or write firewall policies.
407475	`Permission denied` error is shown when an admin user clicked *Create New* in *Traffic Shaping Policy*.
422871	In interface list, when logged in as VDOM admin, the GUI should gray out enable/disable option on interface that does not belong to the admin.
449956	VPN setting should not show IPv6.

Bug ID	Description
458106	*WiFi & Switch Controller* > *FortiSwitch Ports* keeps on spinning.
468003	Not possible to do FW policy search based on an interface name itself when *Interface Pair View* is used.
468314	SD-WAN interface cannot be set as `dstintf` in IPv6 firewall policy.
474524	The GUI policy page won't load for restricted admin.
474737	`fwgrp read&read-write` access profile doesn't work properly.
476237	FortiGate GUI using unsecure telnet to connect to CLI of switches instead of SSH through GUI.
478057	Cannot restore configuration when GUI access to the FortiGate is via a connection with small bandwidth.
478116	Need GUI functionality added back to HUGHES branch for script execution from FortiManager.
481902	When accessing *FortiView* > *Websites* page, gets error *Failed to get FortiView data* and httpsd keeps crashing.
486248	For FG-30D, the default admin has insufficient privileges to access Antivirus profiles in GUI.
487350	*FortiGuard Filtering Services Availability* showing *Unavailable* on GUI when no valid Anti-spam license is present.
487512	Some GUI pages not displayed for administrators who have no access for Web Filter in profile.
488605	*Device Definitions Page* is not loading for a read-only account.
489744	GUI does not allow valid BGP router-id in GUI.
491394	*Network* > *Interfaces* > *Internal error: VDOM*.
494713	Suggest GUI *Disk_Usage_Widget* graph Y-axes scale's maximum unit value to be 100%.
495043	Trusted hosts list is partial within admin details page on GUI and it allows duplicate entries of trusted IPs.
496959	Widgets *Host Scan Summary* and *FortiClient Detected Vulnerabilities* do not count online offnet devices (via WAN).
497427	V3.3.0_533151 remote access stuck loading main dashboard page and login with Fortimanager_ Access user.
501197	Sometimes cannot set or change guest user expiration time in Mozilla Firefox.
501528	Local domain name cannot be removed from GUI, can only be done through CLI.
501982	In POE, POE status not showing and POE port not shown in blue.
503867	In GUI, some certificates break the Certificate page.
504483	DHCP client list for MAC reservation keeps on loading from GUI.
504935	*peertype one* in ikev2 phase1-interface can be chosen in GUI.
505656	When using Edge, a page is reloaded when hovering on a connecting line between objects in the topology.

Bug ID	Description
505985	FortiSwitch Topology in GUI not showing an ISL.
506795	Address object associated virtual pair port is not seen in *Select Entries* dialog box.
506907	Need to improve Dial Codes for Dominican Republic and Puerto Rico.
507427	IP6-mode changed from *delegated* to *static* after some parameter was changed on WebGUI.
508596	GUI Dashboard > Interface Bandwidth widget cannot be added for GRE tunnel interfaces.
512478	If NAT is configured to *Use Outgoing Interface Address* the *Preserve Source Port* switch is hidden or missing.
512481	Cannot see comments on the GUI for VIP GROUPs on FortiOS 6.0.2.

HA

Bug ID	Description
465849	Wrong `diagnose sys ha dump-by vcluster` display when cluster V5.4 and V5.2 are on the same LAN.
502110	`HA-mgmt` interface is displayed on every VDOM.
503118	Slave unit sends several false alert emails everyday after upgrade to 5.6.
506363	Debugzone and checksum output do not match.
510585	HA does not recognize proper ping-server status, hence does not failover when ping-server is down.
512383	`local-in-policy` for `ha-mgmt-int` doesn't work after reboot.

Intrusion Prevention

Bug ID	Description
480525	DHCP doesn't work properly in TP when IPS is enabled.
492193	DoS policies consume 20% more CPU than in FortiOS 5.2.
497602	After upgrading, sniffer packet on `any` interface causes drops on kernel and traffic impact. DoS policies used.
503895	Traffic drops for 15 seconds when UTM is enabled.
505945	IPS `extended-utm-log` `rawdata` log field should include `Url` field.
506234	Cannot configure IPS sensor severity or threat-weight category.
509174	6.0 build 0163 IPSengine 4.021 crash with signal 14.

IPsec VPN

Bug ID	Description
463441	`NAT -T` broken with AWS and FortiGate.
476461	IKE does not release the `mode-cfg framed-IP` assigned from RADIUS.
481720	Using transparent mode and policy base VPN, about 4 ICMP packets which exceed over MTU 1375 byte are dropped.
492366	100% system CPU usage when re-keying idle IPsec tunnels.
502591	Unable to manage FortiGate with FortiManager over IPsec tunnel.
504383	When using the command `get vpn ike gateway` in a VDOM, the firewall CLI session outputs information for only a few tunnels and exits.

Log & Report

Bug ID	Description
490378	Long-live session statistics logs add `sentdelta` and `rcvddelta` fields for FortiCloud and FortiView as required.
500087	Support WCCP set up with one arm WCCP web cache diagram.
503897	FortiGate-501E units generating logs only for five minutes after rebooting the unit, Then do not generate logs anymore.
504238	Incorrect log action blocked even user is "passthrough" in web filter log with warning-prompt per domain.
505474	DNS events are not included in the *security event list*.
507227	All logs in the log disk are erased after upgrading to 6.0.
508277	Non-SIP packet send to SIP ALG gets dropped with no log.

Proxy

Bug ID	Description
497974	WAD crash: signal 11 (Segmentation fault) received everytime when static route is disabled.
500965	In FG-200E kernel conserve mode, WAD process consuming high memory.
503633	Some traffic forwarded to different gateway when proxy based UTM profiles are used.
503667	Numerous WAD process crashes and WAD counter errors.
505772, 513667	WAD process crash with signal 11.
506995	FG-1200D WAD crashing 5.6.5 (WAD MAPI).
507155	System went into conserve mode due to WAD after upgrade to 5.6.5.

Bug ID	Description
511114	WAD crashes when `clientcomfort` is enabled.

REST API

Bug ID	Description
424403	REST API for system CSF didn't return CSF group name.
501749	REST API 403 error on IPS log retrieval with `loggrp.data-access` group.
512038	REST API Post to add address objects to an address group response is incorrect if address group is at max table size.

Routing

Bug ID	Description
490312	When we set keepalive-interval > 0 in GRE tunnel, static route to remote site becomes inactive.
497134	eBGP attempts to reach neighbor via a non-connected route from an IPsec VPN tunnel even though `ebgp-force-multihop` is disabled.
499100	SD-WAN with IPPool not respecting associated interface if one of the links has a dynamic IP.
504164	OSPF - LSA checksum error.
505189	Kernel is missing routes.
505467	For some OSPFv3 intra-area routes, the next-hop link-local address is not displayed.
506074	SD-WAN SLA's restore link value is too small and doesn't account for dynamic routing/convergence.
506627	SD-WAN traffic dropped by tunnel when we create a SD-WAN health check from the HUB.
509988	Dynamic tunnel (shortcut in ADVPN) cannot be established.
511203	When using policy route for IPv6, NAT64 does not work.

SSL-VPN

Bug ID	Description
477231	Unable to log in to VMware vSphere vCenter 6.5 through SSL VPN web portal.
491733	SSL VPN process taking 99% of CPU utilization {tunnel mode only).
492654	`SSLVPND` process crashes and users are disconnected from SSL-VPN.
493772	Some URLs in SSL VPN return `HTTP404`.
496584	SSL VPN bad password attempt causes excessive `bindRequests` against LDAP and lockout of accounts.
499071	SSL VPN logon fails if user is member of a large number of LDAP groups.

Bug ID	Description
499612	Web-mode SSL VPN login attempt fails for user with locally assigned token if GROUP name contains plus(+) sign.
500901	SSL VPN web portal connected to FortiManager (5.6.3) unable to view managed devices and policy packages.
502044	SSL VPN creates user bookmark placeholder where user bookmarks are not allowed.
502365	`SSLVPND` crashes after upgrading from 5.6.3 to 6.0.1.
503160	Unable to render icons via web based SSL VPN bookmark.
503909	Bookmark cannot load successfully in SSL web mode.
506346	JQuery errors when accessing PDF documents through SSL VPN web portal.
507068	Internal server page does not display in SSL VPN web-mode; displays OK in tunnel mode.
507242	Internal web site not working through SSL VPN web mode.
507251	`SSLVPND` is continuously crashing.
510967	Internal server web app not accessible when using SSL VPN web mode and gives error.
512041	SSL VPN users get a JavaScript error when accessing bookmarks in web mode.
512409	In SSL VPN web mode, SMB/CIFS uploaded Japanese file name is garbled.

Switch Controller

Bug ID	Description
504179	Application `cu_acd` has segmentation fault on FortiGate.
510998	Unable to delete SVI on FortiGate and VLAN from switch interface under FortiGate-managed switch after it becomes part of auto-ISL trunk.
511394	Switch-controller `lldp-profile` global limit is hit by creating 500 VDOMs.

System

Bug ID	Description
440411	Monitor NP6 IPsec engine status.
465122	GeoIP database mismatch on cluster after every new database release.
470650	DNS filter getting purged by FortiManager when not used in a policy because FortiGate DNS filter does not contain static entry.
473118	`Fnbamd` crashes after upgrading `ca_bundle` file.
474645	After modifying system settings in GUI, gets wrong message and FGFM status is changed.
476026	Bug in the config revision `diff` function (for comparing two configs).

Bug ID	Description
482497	Running `diagnose npu np6lite session` in FG-201E results in high CPU and system instability.
491090	FortiGuard service is unavalable since upgrading.
495378	Port2 goes down after running for right days on FG-800D.
495493	Central-management settings do not allow push configuration and upgrade versions but do not take effect.
496528	Suggest set IPv6 address as NTP source.
496590	FQDN address object does not accept numbers at the end.
498032	Sometimes 5001E blade crashes during traffic testing with UTM enabled in firewall policy.
499055	DHCPv6c / PD: Single DUID on multiple WAN connections to same carrier causing issues with carrier DHCP utilizing only DUID.
503638	`config system ipip-tunnel` is lost after reboot when using `pppoe` interface.
503725	NP6 affecting all user traffic when enabled on policy.
503751	Changing master 5001E/5001D blade FortiController Trunk Interface MTU setting loses kernel static routes in all slave 5001E/5001D.
504960	Enhancements for maintainer account.
505715	DHCP lease new IP to same EFTPOS S800 device causes DHCP lease exhausted.
505930	FG-3700D freezes when deleting VDOM.
506030	SLBC cluster never in sync after policy push.
506219	Worker blade doesn't update the FT routing cache when phase1 is bound to a loopback interface.
506223	FortiGate is not compliant with RFC 3397 (Domain Search Option Format).
506365	Cannot disable DNS override from CLI, can't disable default gateway from server.
507060	Packet loss on startup when interfaces are in bypass mode.
507061	Longer time to put interfaces in bypass mode during shutdown.
507252	`No session match` for IPsec communication on worker blade master.
507447	FortiGate 300E is bridging OSPF packets during boot phase.
508304	IP is not updating in DDNS with 60D models.
510200	FortiGate DNS configuration doesn't allow single-word domain names.
510419	HTTP link-monitor - response parser is case-sensitive (Content-Length header).
510450	DHCP client is not getting IP address/route in HA A-P context.
512985	Bypass port pairs getting triggered even without any power failure or reboot.
513319	`execute batch start` errors with Cisco ACS tacacs user login.

User & Device

Bug ID	Description
453095	Mobile FortiTokens not assignable VDOM in vcluster on slave unit.
498739	FSSO session interferes with SSL VPN auth sessions, prevents users from accessing allowed destinations.
500426	Email two-factor sending two codes and failing for GUI admin login.
502835	FortiGate reply RADIUS disconnect `nak` to FAC with log of `User name is too long`.
504746	Authenticated users have time-left 49710 days timeout.
509296	WAD user list does not update list based on FSSO.
511108	`ldapconntimeout` allows value which instantly times out LDAP authentication attempts.

VM

Bug ID	Description
484540	FOSVM serial number changes during firmware upgrade.
490248	Virtual disk is automatically divided into three partitions.
497675	No packets received by FortiGate VM virtual NIC when using `type=vhostuser, model=virtio`.
498653	FortiOS VM stops passing traffic after failover.
501190	Fortinet Azure crashes infrequently.
502727	FortiGate VM encounters kernel panic on boot when running on ESXi 6.7.
502881	Cloud native default password and SSH authorized key.
506221	`azd` keep crashing with signal 11.

Web Filter

Bug ID	Description
413187	XFF header enhancements (strip-off & enforcement) for URL filtering module.
482785	Web filter proceed page loading very slowly when setting FortiGuard category to authenticate.
489286	Renaming web filter profile does not take effect.
497075	Fail to retrieve external resource files - Transfer-Encoding: chunked.
500972	Wrong log for FortiGuard block page.
513400	iphone web filter restriction and safe searching do not work.

WiFi Controller

Bug ID	Description
414960	Cannot get crash trace when `hostapd` crashes.
503084	In managed FortiAP, the client filter is not working.
503190	FAP info (`apsn`, `apname`, `channel`, `radioband`) missing from traffic logs.
505439	Local-auth - Missing second RADIUS port from VCFG.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
496642	FortiOS 6.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2018-13371
502940	FortiOS 6.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2018-13374
510148	FortiOS 6.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2018-15473

Known Issues

The following issues have been identified in version 6.0.3. 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.
414172	HTTPsd / DNSproxy / high CPU/memory with high rate UDP 1Byte spoofing traffic.
453610	*Fortiview->Policies(or Sources)->Now*, it 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.
482045	FortiView – no data shown on *Traffic from WAN*.
494731	Incorrect reporting in Fortiview.

GUI

Bug ID	Description
256264	Realtime session list cannot show IPv6 session and related issues.
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.
515983	Firefox cannot list user *TACACS+ Servers*. Chrome is OK.
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).

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.
516033	The traffic log for WANOPT data traffic in the server-side FortiGate should show policy type as *proxy-policy*, not *policy*.

Proxy

Bug ID	Description
516444	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.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the *Device* field.

SSL-VPN

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

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.

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.