FortiOS - Release Notes

Version 6.0.1

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
http://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

October 19, 2018
FortiOS 6.0.1 Release Notes
01-601-489174-20181019

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-06-05	Initial release.
2018-06-06	Added FG-94D-POE to *Introduction* > *Supported models* > *FortiGate* and removed *FGT-94D-POE reboot and factory reset* from *Special Notices*.
2018-06-08	Added 482835 to *Known Issues*.
2018-06-11	Moved 482835 to *Resolved Issues*.
2018-06-20	Deleted *Upgrade Information* > *FortiGate-VM64-Azure upgrade*.
2018-06-26	Added 476125 to *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2018-07-06	Updated *Upgrade Information* > *Physical interface inclusion in zones* section.
2018-10-19	Added *Bandwidth and session counts from FortiAnalyzer units running older versions* to *Special Notices*. Updated 485676 in *Resolved Issues*. Updated *Upgrade Information* > *FortiGuard update-server-location setting*.

Introduction

This document provides the following information for FortiOS 6.0.1 build 0131:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.1 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-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-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, 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 6.0.1 images are delivered upon request and are not available on the customer support firmware download page.

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 mode:

- 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.

Bandwidth and session counts from FortiAnalyzer units running older versions

When using FortiOS 6.0.1 with FortiAnalyzer units running 5.6.5 or lower, or 6.0.0/6.0.1, 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

Upgrading to FortiOS 6.0.1

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

If you are upgrading from version 5.6.2 or 5.6.3, this caution does not apply.

Before upgrading, ensure that port 4433 is not used for `admin-port` or `admin-sport` (in `config system global`), or for SSL VPN (in `config vpn ssl settings`).

If you are using port 4433, you must change `admin-port`, `admin-sport`, or the SSL VPN port to another port number before upgrading.

Physical interface inclusion in zones

Upgrading from 5.6.3 or later removes all of the members of a zone if the zone contains a physical interface and at least one of that physical interface's VLAN interfaces is removed. For example:

Before Upgrade:

```
config system zone
   edit "Trust"
   set interface "port1" "Vlan01" "Vlan02" "Vlan03"
next
```

After Upgrade:

```
config system zone
   edit "Trust"
next
```

Remove `"port1"` from the list and the upgrade will retain the VLANs.

Conditions when physical zone members are removed:

- If a physical interface has a VLAN associated (regardless of whether they are in the same zone or any zone)

Conditions when VLAN zone members are removed:

- If the parent physical interface is also set on a zone

You can use the following options to prepare for the upgrade:

- Use only physical interfaces that have no VLAN associations

  Or:
- Create new VLANs in place of current physical interface zone members, and remove all physical zone members from zones using only the associated, new VLAN entries.

Fortinet Security Fabric upgrade

FortiOS 6.0.1 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 6.0.1. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.1 and some running 5.6.x.

Minimum version of TLS services automatically changed

Support for TLS 1.0 has been discontinued for improved security. Going forward, only TLS 1.1 and TLS 1.2 will be supported.

When you upgrade to FortiOS 6.0.1 and later, all SSL and TLS services using 1.0 are automatically upgraded to 1.1 or later. For example, the `ssl-min-version` option automatically changes during upgrade to FortiOS 6.0.1 and later. As a result, if you are using TLS 1.0 with older versions of FortiOS, you can no longer use it with FortiOS 6.0.1 and later.

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 6.0.1 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 6.0.1 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 `any`.

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

FortiOS 6.0.1 support

The following table lists 6.0.1 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 Fortinet Security Fabric upgrade on page 11. 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 Fortinet Security Fabric upgrade on page 11. 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 FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate. 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 0267 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	• 4.00017
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, and 2012 R2
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	2336. Download from the Fortinet Developer Network https://fndn.fortinet.net.

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

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

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

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
OS X El Capitan 10.11.1	Apple Safari version 9 Mozilla Firefox version 54 Google Chrome version 59
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 6.0.1. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
451348	Flow AV SSL traffic EICAR detection failure.
481615	MMDB has random version number after upgrading from 5.6.3 to 6.0.
481785	Regular AVDB becomes 1.00000 after rebooting FortiGate.

Authentication & User

Bug ID	Description
483553	In case there are multiple LDAP search results for the same LDAP search query, LDAP group match fails.

Connectivity

Bug ID	Description
474630	Central Management: IP/Domain Name disappears when using FQDN and clicking **Apply** brings down management tunnel.
477135	Updates of FortiGuard are causing CPU spikes slowing down the regular traffic.

Firewall

Bug ID	Description
463468	Clients are unable to connect to the mail server when WAF is enabled on the VIP policy.
479672	FortiTelemetry not blocking VIP.

FortiGate 90D

Bug ID	Description
482835	The `cu_acd` process uses high CPU on FG-90D.

FortiView

Bug ID	Description
439438	FortiView time line for system events.

GUI

Bug ID	Description
306406	FortiSwitch Ports page display improvements.
389328	REST API uses incorrect access group for backup and restore config.
389747	*Shaping Policy* dialog: should hide warning message when profile group contains app control used in policy.
389794	Simplify GUI proxy options based on inspection mode, and make the dialog/list consistent.
392569	New dashboard *Sensor Information* widget power supply value is incorrect.
397979	Dynamic Malware Detection version shows *not loaded*, even when the information is retrieved from FortiCloud.
451029	Should be able to assign hard token to user with no email configured by using the right-click menu.
454734	Security Fabric topology page cannot show detected server for (client) LAN > LAN (server) traffic.
455169	Dialup VPN phase2 selector name doesn't display on GUI.
458546	LDAP user credential test in GUI gives `syntax error`. In CLI, user credential test works OK.
462279	New muTable list to support showing total count for matching entries.
462487	GUI should show all admin trusted hosts not just show the first three items.
464211	Some words are cut off when change widget is resized to 1X1 on dashboard.
464211	Some words cut off when changing widget size to *1*1* on dashboard.
468530	Can't set 2FA authentication and email recipient with `admingrp&usergrp` read-write on GUI.
469666	While creating a local user, FortiGate GUI freezes, PC browser memory usage spikes, and the user is not created.
469807	Newly added app-ctl list entry cannot be found in drop-down menu on GUI until reboot.
470215	Selecting an interface with a name like *a.b* for SD-WAN will not show stats or connection information in *Performance SLA*.
472037	Changing disk usage in GUI fails.
472390	GUI won't load with ECC certificate selected.
473086	Quarantine monitor should support showing devices for the whole fabric.

Bug ID	Description
473140	Cannot paste a script or any character in the GUI CLI console.
473791	Four duplicate entries are displayed in WANOPT peer monitor when one peer was configured.
474538	Remove mobile malware protection option from GUI.
474548	Remove *mobile malware protection* option from GUI.
474775	Downstream FortiGates intermittently disappear from *Security Fabric* widget.
477496	Unable to add email wildcard to black/white list GUI in Anti-Spam profile.
477592	Data shown under incorrect date in *Logs Sent to FortiAnalyzer Daily* graph.
477748	Add a one-click launch button or Link on FortiOS GUI to help user start a FortiSandbox in AWS.
479030	Should remove *Any* interface in SD-WAN rule when you specify one or more interfaces.
480544	The *Policy Edit Dialog* shows *WAN-OPT* and *Web Cache* options even though *Disk Setting* is set at *Log*.
480857	In some configurations, the interface page cannot be displayed when logged in as prof admin.
480910	Cannot configure and display interface comments on GUI.
480931	GUI shows wrong expiry time when interface mode is DHCP.
481031	Cannot set Security Fabric automation destination to multiple FortiGates in GUI when creating and editing automation.
481373	*Security Rating* in multiple FortiGates always shows first percentile even when they get different security rating scores.
481381	Industry field shows up abnormally when adding security rating widget.
481388	The radio button for *Enable Explicit FTP Proxy* is off in the interface editing page even though FTP proxy is enabled.
481436	GUI cannot assign remote-ip for site-to-site IPsec tunnel interface.
481563	The log viewer cannot view and download IPS archive when device is FortiAnalyzer and archive panel is blank.
481663	Get `Error 500` message when editing one-arm sniffer if including IPv6 Packets.
481797	*Policy View/Log View*: missing tooltip when mouse over policy ID.
482679	FortiCare registration from GUI does not work.
482689	Cannot change password or log out of GUI when logged in as guest admin.
484246	Could not show *Application Control* and *WebFilter* log in GUI under *NGFW policy* mode.
492784	Could not add application, app, and URL category for traffic shaping policy from GUI in policy.

HA

Bug ID	Description
474867	FortiGate does not send syslog from `ha-mgmt-interface` after `management-vdom` is changed.
480932	New factory reset box fails to sync with master in multi-VDOM after upgrade. Workaround: reboot the new slave.

IPS

Bug ID	Description
230766	Flow-AV full mode should support archive block/log feature.
421854	Increase number of custom signatures allowed.
451452	IPS Engine signal 14 alarm clock crash on FGT90D.
460138	When upgrading IPS engine to anything higher than 3.174, Google applications sometimes get blocked.
469608	ICMP packets dropped during FortiGate update.
481107	IPS Engine signal 11 crash during stress test.

IPsec VPN

Bug ID	Description
469648	Not all IPv6 IPsec VPN traffics works properly when crossing NP6.
471326	AES-256-GCM for phase 1.
474408	Multicast resolve wrong OIF for dialup VPN using `exchange-ip` to assign address (net-device enable).
481153	IPsec configuration can't create (no pask) when re-enabling OCVPN after FortiGate factory reset.
481449	OCVPN may not work if FortiGate hostname is different from the one registered on cloud.
482622	Traffic selector issues with IKEv2 in transport-mode and NAT.
482622	Traffic Selector issues with IKEv2 in transport-mode and NAT.

Log & Report

Bug ID	Description
455193	Flow-based webfilter URL exempt not generating a UTM log.

Bug ID	Description
474867	FortiGate does not send syslog from `ha-mgmt-interface` after `management-vdom` is changed.
476575	Filter `result` fields on compliance-check event log not working.
477411	Update the *Meaning* field in the logging module.
477592	Data shown under incorrect date in *Logs Sent to FortiAnalyzer Daily* graph.
489065	When user authentication/authorization fails, username should be logged in the user event log.

Router

Bug ID	Description
472512	FortiGate not forwarding DNS packets when policy route is hit and DNS filter profile applied to firewall policy.
480978	OSPF summary-address synchronized with FGSP.
483443	VRRP start time option does not work when the VRRP primary device interface goes from down to up.

Security Fabric and Rating

Bug ID	Description
481373	Security rating widget in multiple FortiGates always show first percentile even if they get different security rating scores.
465756	Automation should be available even when Security Fabric is not enabled.

Spam

Bug ID	Description
466606	Emails tagged as SPAM - Whitelist is not effective.

SSL VPN

Bug ID	Description
456027	SMB bookmark in SSL VPN portal doesn't work with dynamic user-mapping and gets `Invalid HTTP request` error.
466821	Accessing *Cisco Unified Communications Manager* not working properly.
483253	FQDN doesn't work well through SSL VPN web mode.
484381	SSL VPN portal URL unreserved characters encoding issue.

System

Bug ID	Description
379015	Encounter `forticron signal 11` crash after changing VCPU allocation to above 82 cores.
388563	`snmpd signal 6` crash frequently in corporate firewall 3700D
415910	CPU cores utilization shows 0% while handling CPS in 5.4.
435910	On FG-50E and FG-51E, `ifHCOutOctets` rolls at counter32.
464332	SNMP agent returns `No Such Object available` when querying `etherStatsCRCAlignErrors` MIB variable.
464332	SNMP Agent returns *No Such Object available* when querying `etherStatsCRCAlignErrors` MIB variable.
469608	ICMP Packets drop while FGD updates.
471626	`dot3StatsFCSErrors` MIB OID query systematically returns `0` despite CRC errors recorded in `rx_crc_error` counter.
471626	`dot3StatsFCSErrors` MIB OID query systematically returns `0` despite CRC errors recorded in `rx_crc_error` counter.
472195	Request to increase `Strict-Transport-Security` HTTP Header `max-age=` value or make it configurable to pass security audit.
474630	If using FQDN, in *System* > *Settings*, *Central Management*, the *IP/Domain Name* disappears when clicking *Apply* and this causes management tunnel to go down.
474833	Newly-generated *Fortinet_CA_SSL* certificate reverts back to previous version after reboot, on FG-61E with VDOMs.
477135	Updates of FortiGuard causes CPU spikes that slow down regular traffic.
477670	FortiGate 100E stops processing traffic and responding to management on HTTP, HTTPS, SSH, ping, etc.
477979	Potential memory leak detected in FTS.
477979	Potential memory leak detected in FTS.
479611	Cannot set the port associated with firewall address to virtual wire pair.
479611	Cannot set the port that is associated with firewall address to virtual wire pair.
480015	Cannot show full configuration if used before entering global,
480831	Wrong interface status and no info on system panel after logging in with VDOM admin.
481768	SIP ALG is not properly applying NAT.
483516	FG-81 enters conserve mode suddenly and scanunit process crashes.
489450	TCP traffic cannot go through NP6Lite with Nturbo enabled.

Upgrade

Bug ID	Description
481085	Tolerance of `vpn ssl web portal` lost when upgrading from 5.6.3 to 6.0.0.
481146	`ssl-min-version` of virtual server changed to `tls-1.1` during upgrade from 5.6.3.

VM

Bug ID	Description
477748	Add a one-click launch button or link on FOS GUI to help user start a FortiSandbox in AWS.
480860	FGT_VM with evaluation license does not run security rating.
485676	Upgrading FortiGate VM from 5.6.3 to 6.0.0 changes `update-server-location` setting to `usa`.

WanOpt & Webcache

Bug ID	Description
464434	WAN OPT is unavailable in FGT-VM GUI even when disk usage is set to `wanopt`.

Web Filter

Bug ID	Description
472512	FortiGate not forwarding DNS packets when policy route is hit and DNS filter profile is applied to firewall policy.
484556	URL filter does not match for right-hand matched URL when there is similar URL entry which includes a dash (-).

WebProxy

Bug ID	Description
459504	File upload does not work on FTP over HTTP when security profile is configured.
469656	WAD is crashing at signal 11.
471664	FG-1500D goes into kernel conserve mode. WAD process consumes high memory.
480722	WAD crashes at signal 11.
481649	With user authentication, the fourth request for FTP proxy service in a row is blocked.
482948	WAD daemon has signal 11 crash twice on corporate firewall.
484983	WAD SSL proxy crashes with signal 11.

WiFi

Bug ID	Description
449137	FWF-xxE series local radio working as monitor mode cannot suppress rogue ap/sta.
478458	PMF on SSID causes application `hostapd (wpad_ac)` crash.
481394	Fast BSS Transition on SSID causes `wpad_ac` high CPU usage (FAP cannot be managed).
482970	FAP with MAC OUI 70-4C-A5 as mesh leaf cannot connect with FWF local radio as mesh root.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
476125	FortiOS 6.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2018-9185

Known Issues

The following issues have been identified in version 6.0.1. 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.

Authentication & User

Bug ID	Description
477392	Cannot use FAC username password and FortiToken two-factor authenticate login HA slave unit.
491175	`diag test application fnbamd 1` causes `fnbamd` to enter an idle state and causes authentication failure.
491241	Enhance diag command `diag test app fnbamd 1`.

Connectivity

Bug ID	Description
481058	Configuration revision control list can't be retrieved from FortiCloud.

DLP

Bug ID	Description
478524	Diskless model missing `full-archive-proto` in config DLP sensor when only FortiCloud logging enabled.

Firewall

Bug ID	Description
474612	SNAT is using low ports below 1023.
492961	Set `utm-status disable` did not hide profile-group. Unset `profile-group` will make `profile-protocol-options` empty.

FortiGate 3815D

Bug ID	Description
385860	FG-3815D does not support 1GE SFP transceivers.

FortiSwitch-Controller/FortiLink

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

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.
449598	*Remote LDAP User Definition* wizard does not pull users.
451776	Admin GUI has limit of 10 characters for OTP.
468797	Cannot filter by date or timestamp when viewing logs from FortiCloud.
470241	Raw logs are downloaded from the default location even if you select another log device in GUI.
470589	The *Forward Traffic Log Details* panel *Security* tab does not display security log details when multiple log devices are enabled.

Bug ID	Description
472023	Outbreak prevention detection makes "clean" counter increment in *Advanced Threat Protection Stats* widget.
473808	Column filter is not persistent and is removed after refreshing the page.
479468	The link status is lost after SD-WAN GUI changes to *List Edit*.
481902	When accessing *FortiView* > *Websites* page, gets error *Failed to get FortiView data* and httpsd keeps crashing.
487350	*FortiGuard Filtering Services Availability* showing *Unavailable* on GUI when no valid Anti-spam license is present.
489674	When scroll to the end of an muTable, GUI should shows 100% of entry.
492898	Cannot delete FSSO AD group entries in GUI anymore.
493351	Object tooltip of last page should not always display on current page.
493839	Cannot change quota type (time-based, traffic-based).
494040	Creating/Modifying security profiles generates multiple logs with misleading action.
494724	When creating trunk interface on managed FSW, FSW ports in right-side list show down, even when some are up.

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).
482548	Conserve mode caused by `hasync` consuming most of memory.
493759	When `vcluster2` is removed from HA config, all active sessions are killed once `session-ttl` is reached.
494029	After failover, sometimes cannot connect to *management-ip* of backup device.

IPS

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.
486552	vcluster HA failover fails with large site-to-site IPsec VPN configuration on 3800D.

Log & Report

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

Security Fabric

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

SSL VPN

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

System

Bug ID	Description
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
364280	User cannot use `ssh-dss` algorithm to login to FortiGate via SSH.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
440411	Monitor NP6 IPsec engine status.
460617	GUI FortiGuard *Check Again* button doesn't work as expected due to FortiGuard service 8888/53 incorrectly routed.
466048	Huawei USB LTE E3276 cannot be detected.
468684	EHP drop improvement for units using `NP_SERVICE_MODULE`.

Bug ID	Description
472843	When FMG is set for `DM = set verify-install-disable` FGT does not always save script changes.
474132	FG-51E hang under stress test since build 0050.
475539	Inaccurate netflow export. Traffic measurements do not match with SNMP readings.
477870	Alias for modem interface present in GUI but not in CLI.
482497	Running `diagnose npu np6lite session` in FGT-201E results in high CPU and system instability.
494042	If we create VLAN in VDOM A, then we cannot create ZONE name with the same VLAN name in VDOM B.
494603	FortiGate in transparent mode is not accessible over https/ssh (administrative access) once trusted host is configured.

Upgrade

Bug ID	Description
470575	After upgrading from 5.6.3, `g-sniffer-profile` and `sniffer-profile` exist for IPS and webfilter.
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.

VM

Bug ID	Description
491974	Possible memory leak in `awsd`.

Web Filter

Bug ID	Description
480003	FortiGuard category does not work in NGFW mode policy.
486171	The *Web Rating Overrides* option doesn't work with flow-mode.
490377	The *Web Rating Overrides* option doesn't work properly on proxy-based.

Webproxy

Bug ID	Description
474296	High memory usage on WAD process.
491424	Adjust the `proxy-auth-timeout` default value and unit.
491630	With UTM enabled, client failed to get response from server, gets 500 Internal error.

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.