FortiOS - Release Notes

Version 6.0.10

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

June 18, 2020
FortiOS 6.0.10 Release Notes
01-6010-640265-20200618

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-06-18	Initial release.

Introduction

This document provides the following information for FortiOS 6.0.10 build 0365:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.10 supports the following models.

FortiGate	FG-30D, FG-30D-POE, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG- 200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3400E, FG-3401E, FG3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN, FG-VM64-GCP, FG-VM64-OPC, FG-VM64-GCPONDEMAND
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 6.0.10 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 6.0.10. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0365.

FG-30E-MG	is released on build 5459.
FG-60F	is released on build 6812.
FG-61F	is released on build 6812.
FG-100F	is released on build 6812.
FG-101F	is released on build 6812.
FG-1100E	is released on build 6801.
FG-1101E	is released on build 6801.
FG-2200E	is released on build 6803.
FG-2201E	is released on build 6803.
FG-3300E	is released on build 6803.
FG-3301E	is released on build 6803.
FG-VM64-AZURE	is released on build 5455.
FG-VM64-AZUREONDEMAND	is released on build 5455.
FG-VM64-RAXONDEMAND	is released on build 8938.
FWF-60F	is released on build 6812.
FWF-61F	is released on build 6812.

Special Notices

WAN optimization and web caching functions

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

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

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

FortiGuard Security Rating Service

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

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

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

Using FortiManager as a FortiGuard server

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

Built-in certificate

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

FortiGate and FortiWiFi-92D hardware limitation

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

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

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

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

When the command is enabled:

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

When the command is disabled:

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

FG-900D and FG-1000D

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

FortiClient (Mac OS X) SSL VPN requirements

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

FortiClient profile changes

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

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

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

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

Using FortiAnalyzer units running older versions

When using FortiOS 6.0.10 with FortiAnalyzer units running 5.6.5 or lower, or 6.0.0-6.0.2, FortiAnalyzer might report increased bandwidth and session counts if there are sessions that last longer than two minutes.

For accurate bandwidth and session counts, upgrade the FortiAnalyzer unit to the latest version.

L2TP over IPsec on certain mobile devices

Bug ID	Description
459996	Samsung Galaxy Tab A 8 and Android 9.0 crash after L2TP over IPsec is connected.

Upgrade Information

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

To view supported upgrade path information:

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

FortiGuard protocol and port number

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

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

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

Fortinet Security Fabric upgrade

FortiOS 6.0.10 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.0.8
- FortiClient EMS 6.0.8
- FortiClient 6.0.9
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.9 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.0.10. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.10 and some running 5.6.x.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.0.10 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 6.0.10 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 6.0.10 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 6.0.10 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
```

External IP not allowed to be the same as mapped IP

Traffic will be dropped when the IPS is enabled in a policy with a VIP that has the same external and mapped IP.

To avoid this, the kernel will disallow the configuration of the same `extip` and `mappedip` for VIPs in the CLI starting from FortiOS 6.0.0.

Product Integration and Support

The following table lists FortiOS 6.0.10 product integration and support information:

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

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0291 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2008 Core
	  • Novell eDirectory 8.8

FortiExtender	• 3.3.2, 4.0.0
AV Engine	• 6.00027
IPS Engine	• 4.00061
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04 (32-bit & 64-bit)	2336. Download from the Fortinet Developer Network: https://fndn.fortinet.net.

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

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

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

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 66 Google Chrome version 73
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 66 Google Chrome version 73
Linux Ubuntu 16.04 / 18.04 (32-bit & 64-bit)	Mozilla Firefox version 66
MacOS High Sierra 10.13.6	Apple Safari version 12 Mozilla Firefox version 66 Google Chrome version 72
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

SSL VPN host compatibility list

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

Supported Microsoft Windows XP antivirus and firewall software

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

Supported Microsoft Windows 7 32-bit antivirus and firewall software

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

Resolved Issues

The following issues have been fixed in version 6.0.10. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
553143	Redundant logs and alert emails sent when file is sent to FortiSandbox Cloud via *Suspicious Files Only*.
560044	Secondary device blades occasionally report critical log event `Scanunit initiated a virus engine/definitions update`.
561524	Cannot send an email with PDF attachment when FortiSandbox Cloud inspection is enabled.
562037	CDR does not disarm files when they are sent over HTTP POST, despite AV logs showing file has been disarmed.
563250	Shared memory not emptying out properly under /tmp.
581460	FG-30E AV TP mode cannot log and block oversize files.

Data Leak Prevention

Bug ID	Description
563447	Cannot download DLP archived file from GUI for HTTPS, FTPS, SMTP and SMTPS.
607444	DLP quarantines IP when no quarantine action is configured.

Explicit Proxy

Bug ID	Description
603707	The specified port configurations of `https-incoming-port` for `config web-proxy explicit` disappeared after rebooting.

Firewall

Bug ID	Description
597110	When creating a firewall address with the `associated-interface` setting, cmd will stuck if there is a large nested `addrgrp`.
604886	Session stuck in proto_state=61 only when flow-based AV is enabled in the policy.
611840	Firewall policy search with decimal in the name fails in GUI.

GUI

Bug ID	Description
574101	Empty firmware version in *Managed FortiSwitch* GUI page.
586604	No matching IPS signatures are found when the *Severity* or *Target* filters are applied.

HA

Bug ID	Description
531083	Configuration of HA pair of FortiGates goes out of sync when removed from central management (FortiManager).
540632	In HA, `management-ip` that is set on a hardware switch interface does not respond to ping after executing reboot.
586004	Moving VDOM via GUI between virtual clusters causes cluster to go out of sync and VDOM state work/standby does not change.
621621	Ether-type HA cannot be changed.

Intrusion Prevention

Bug ID	Description
540718	Signal 14 alarm crashes were observed on DFA rebuild.
579018	IPS engine 5.030 signal 14 alarm clock crash at `nturbo_on_event`.
608501	IPS forwards attacks that are previously identified as dropped.

IPsec VPN

Bug ID	Description
516029	Remove the IPsec global lock.
532594	IKED crashed using ADVPN and OSPF.
602240	IKEv2 EAP-TLS handshake detected retransmit of client, but FortiGate does not retransmit its response.
604923	IKE memory leak when IKEv2 certificate subject alternative name/peer ID matching occurs.
612319	MTU calculation of shared dynamic phase 1 interface is too low compared to its phase 2 MTU and makes fragmentation high.

Log & Report

Bug ID	Description
531994	User group is not included in traffic log for transparent web proxy policy when traffic is allowed.
608565	FortiGate sends incorrect long session logs to FortiGate Cloud.

Proxy

Bug ID	Description
578251	Download bandwidth under FortiView is not accurate when traffic is being inspected by proxy mode AV.
622818	Breakout traffic is wrongly denied by proxy policy.

Routing

Bug ID	Description
560633	OSPF route for ADVPN tunnel interface flaps.
593864	Routing table is not always updated when BGP gets an update with changed next hop.
600332	SD-WAN GUI page bandwidth shows *0* issues when there is traffic running.
630758	When an obsolete ISDB ID is used in a static route, a default route is created after rebooting.

SSL VPN

Bug ID	Description
476377	SSL VPN FortiClient login with FAC user FTM two-factor fail because it times out too fast.
525106	HTML PABX Admin Console not working correctly in SSL VPN mode.
525342	In some special cases, SSL VPN main state machine reads function pointer is empty that will cause SSL VPN daemon crash.
556657	Internal website not working through SSL VPN web mode.
561585	SSL VPN does not correctly show Windows Admin center application.
563022	SSL VPN LDAP group object matching only matches the first policy; is not consistent with normal firewall policy.
573853	TX packet drops on SSL root interface.
574724	In some lower-end FortiGates, the threshold of available memory is not calculated correctly for entering SSL VPN conserve mode. Threshold should be 10% of total memory when the memory is larger than 512 MB and less than 2 GB.
577522	SSL VPN daemon crashes when logging in several times with RADIUS user that is related to a framed IP address.
582265	RDP sessions are terminated (disconnect) unexpectedly.
588066	SSO for HTTPS fails when using "\" (backslash) with the domain\username format.
596441	FortiOS does not correctly re-write the Exchange OWA logoff URL when accessed via SSL VPN bookmark.
597658	Internal custom web application page running on Apache Tomcat is not displaying in SSL VPN web mode.
599394	SSL VPN web portal bookmarks are not full loading for Vivendi SelfService application.
600029	Sending RADIUS accounting interim update messages with SSL VPN client framed IP are delayed.
601084	Site in .NET framework 4.6 or 4.7 not loading in SSL VPN web mode.
601867	SSL VPN web mode cannot open DFS share subdirectories, gives invalid HTTP request message.
604772	SSL VPN tunnel is unexpectedly down sometimes when certificate bundle is updated.
610564	RDP over web mode SSL VPN to a Windows Server changes the time zone to GMT.
619306	SSL VPN daemon crash when multiple sessions are conflicting.
621270	SSL VPN user groups are corrupted in auth list when the user is a member of more than 100 groups.
622110	SSL VPN disconnects when importing or renaming CA certificates.
635240	The SSL VPN connection is not empty after destroying it, so it may be reused and crashes.

System

Bug ID	Description
511790	Router info does not update after plugging out/plugging in USB modem.
544570	Primary unit does not send SNMP trap for all SNMP servers when plugging out the cable from the LAG configured interface.
567019	CP9 VPN queue tasklet unable to handle kernel NULL pointer dereference at 0000000000000120 and device reboots.
569652	High memory utilization after upgrading FortiOS and IPS engine.
580038	Problems with cmdbsvr while handling a large number of FSSO address groups and security policies.
581496	FG-201E stopped sending out packets; NP6lite is stuck.
581528	SSH/RDP sessions are terminated unexpectedly.
582536	Link monitor behavior is different between FGCP and SLBC clusters.
587911	FortiGate 200D is dropping packets.
592827	FortiGate is not sending DHCP request after receiving offer.
604613	`sentbyte` of NTP on local traffic log shows as `0` bytes, even though NTP client receives the packet.
607452	Automatically logged out of CLI when trying to configure STP due to /bin/newcli crash.
608442	After a reboot of the PPPoE server, the FortiGate (PPPoE clients, 35 clients) keeps flapping (connection down and up) for a long time before connecting successfully.
610604	hasync and cmdbsvr processes crash on secondary unit, causing failed httpsd, fgfmd, and snmpd on the primary unit.
610900	Low throughput on FG-2201E for traffic with ECN flag enabled.
612351	Many `no session matched` logs while managing FortiGate.
614355	VPN interface is not pingable while NPU is enabled (FG-60F/61F).
616022	Long delay and cmdbsvr at 100% CPU consumption when modifying address objects and address groups via GUI or REST API.
617409	The FG-800D HA LED is off when HA status is normal.
636069	Unable to handle kernel NULL pointer dereference at 000000000000008f.

User & Device

Bug ID	Description
538925	Collector agent cannot be contacted after rebooting or restarting authd if FQDN is used on FSSO server.
586334	Brief connectivity loss on shared service when RDP session is logged in to from local device.
587293	The session to the SQL database is closed as `timeout` when a new user logs in to terminal server.
597884	Global imported local certificates can no longer be used in VDOMs.
605437	FortiOS does not understand CMPv2 `grantedWithMods` response.
605950	RDP sessions are terminated (disconnect) unexpectedly.

VM

Bug ID	Description
614038	vMotion causing sessions to be disconnected as it consider sessions stateless.

VoIP

Bug ID	Description
620742	RAS helper does not NAT the port 1720 in the `callSignalAddress` field of the `RegistrationRequest` packet sent from the endpoint.

Web Filter

Bug ID	Description
510509	Static `urlfilter` changes do not always work properly or take immediate effect.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
558685	FortiOS6.0.10 is no longer vulnerable to the following CVE Reference: • CVE-2020-12812
576090	FortiOS 6.0.10 is no longer vulnerable to the following CVE Reference: • CVE-2019-17655

Known Issues

The following issues have been identified in version 6.0.10. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
590092	Cannot clear `scanunit vdom-stats` to reset the statistics on ATP widget.

Firewall

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

FortiView

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

Log & Report

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

Proxy

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

System

Bug ID	Description
609668	VLANs under LAGs do not show RX/TX packets.

User & Device

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

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.