FortiOS - Release Notes

Version 6.2.7

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

December 17, 2020
FortiOS 6.2.7 Release Notes
01-627-682193-20201217

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-12-17	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 6.2.7 build 1190.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.7 supports the following models.

FortiGate	FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30E-MG, FG-40F, FG-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, 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-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, 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-40F, FWF-40F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-30D, FGR-35D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 6.2.7. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1190.

FG-80F	is released on build 5970.
FG-80F-BP	is released on build 5970.
FG-81F	is released on build 5970.

FG-100F	is released on build 5978.
FG-101F	is released on build 5978.
FG-200F	is released on build 6865.
FG-201F	is released on build 6865.
FG-400E-BP	is released on build 5968.
FGR-60F	is released on build 5977.
FGR-60F-3G4G	is released on build 5977.

Special notices

New Fortinet cloud services

FortiOS 6.2.0 introduced several new cloud-based services listed below. The new services require updates to FortiCare and Fortinet's FortiCloud single sign-on (SSO) service.

- Overlay Controller VPN
- FortiGuard Cloud-Assist SD-WAN Interface Bandwidth Monitoring
- FortiManager Cloud
- FortiAnalyzer Cloud

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
- FGR-35D
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E
- FGT-51E
- FGT-52E
- FWF-30E

- FWF-30E-MI
- FWF-30E-MN
- FWF-50E
- FWF-50E-2R
- FWF-51E

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.

FortiGate 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 does 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.

CAPWAP traffic offloading

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. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

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

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.

NP4lite platforms

FortiOS 6.2 and later does not support NP4lite platforms.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

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.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`:
  - in FortiOS 6.2.6 and later, set `unsupported-ssl` to `block`.
  - in FortiOS 6.4.3 and later, set `unsupported-ssl-negotiation` to `block`.

New features or enhancements

Bug ID	Description
654032	The `route-tag` is a mechanism to map a BGP community string to a specific tag. The string may correspond to a specific network that a BGP router advertised. With this tag, an SD-WAN service rule can be used to define specific traffic handling to that network. IPv6 route tags are now supported.

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*.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.2.7 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.2.5
- FortiClient EMS 6.2.3 and later
- FortiClient 6.2.3 and later
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.11 and later

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC

If the Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.7. When the Security Fabric is enabled in FortiOS 6.2.7, all FortiGate devices must be running FortiOS 6.2.7.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.7 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.2.7 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.2.7 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.2.7 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.2.7, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.2.7.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

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
```

FortiView widgets

FortiView widgets have been rewritten in 6.2.7. FortiView widgets created in previous versions are deleted in the upgrade.

Product integration and support

The following table lists FortiOS 6.2.7 product integration and support information:

Web Browsers	• Microsoft Edge 44 • Mozilla Firefox version 76 • Google Chrome version 81 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 76 • Google Chrome version 81 • Microsoft Internet Explorer version 11 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 13. 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 13. 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**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 13 and Fortinet Security Fabric upgrade on page 13. 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	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 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
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 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 0295 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • 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	• 4.1.2
AV Engine	• 6.00154
IPS Engine	• 5.00229
Virtualization Environments	
Citrix	• Hypervisor Express 8.1, build 2019-12-04
Linux KVM	• Ubuntu 18.04.3 LTS • QEMU emulator version 4.4.4 (Debian 1:4.0+dfsg-0ubuntu9.4) • libvirtd (libvirt) 4.0.0
Microsoft	• Hyper-V Server 2019
Open Source	• 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 X520

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 / 18.04 (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 76 Google Chrome version 81
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 76 Google Chrome version 81
Linux CentOS 7/8	Mozilla Firefox version 68
OS X Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 76 Google Chrome version 81
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 6.2.7. For inquires about a particular bug, please contact Customer Service & Support.

Firewall

Bug ID	Description
651321	`sflowd` is crashing due to invalid custom application category.

GUI

Bug ID	Description
656429	Intermittent GUI process crash if a managed FortiSwitch returns a reset status.

HA

Bug ID	Description
616345	Secondary device failed to sync with primary device when FGSP is peer configured, but hasync fails to bind socket.
671737	HA is not syncing after upgrading to 6.2.5 due to failure to bind socket.

Intrusion Prevention

Bug ID	Description
668631	IPS is constantly crashing, and `ipshelper` has high CPU when IPS extended database has too many rules (more than 256) sharing the same pattern. Affected models: SoC3-based FortiGates.

IPsec VPN

Bug ID	Description
610203	When an offloaded IPsec SA uses NP6 reserved space, it gets stuck and packets on the tunnel start to drop.
645196	Static routes added by iked in non-root VDOM are not removed when tunnel interface status is set to down by configuration change.
663126	Packets for the existing session are still forwarded via the old tunnel after the routing changed on the ADVPN hub.
668554	Upon upgrading to FortiOS 6.2.6, a device with IPsec configured may experience IKE process crashes when any configuration change is made or an address change occur on a dynamic interface.
670025	IKEv2 `fragmentation-mtu` option is not respected when EAP is used for authentication.
673258	FortiGate to Cisco IKEv2 tunnel randomly disconnects after rekey.

Log & Report

Bug ID	Description
651581	FortiGate tried to connect to FortiGate Cloud with the primary IP after reboot, although the secondary IP is the source in the FortiGuard log.

Routing

Bug ID	Description
654032	SD-WAN IPv6 route tag command is not available in the SD-WAN services.
661769	SD-WAN rule disappears when an SD-WAN member experiences a dynamic change, such as during a dynamic PPPoE interface update.
668982	Possible memory leak when BGP table version increases.
670017	FortiGate as first hop router sometimes does not send register messages to the RP.
672061	In IPsec topology with hub and ~1000 spokes, hundreds of spoke tunnels are flapping, causing BGP instability for other spokes.

Security Fabric

Bug ID	Description
631607	CSF root FortiGate cannot listen on loopback interface.
669436	Filter lookup for Azure connector in subnet and virtual network does not show all results.

SSL VPN

Bug ID	Description
664121	SCM VPN disconnects when performing an SVN checkout.
666194	WALLIX Manager GUI interface is not loading through SSL VPN web mode.
667780	Policy check cache should include user or group information.
669685	Split tunneling is not adding FQDN addresses to the routes.
669707	The jstor.org webpage is not loading via SSL VPN bookmark.
670803	Internal website, http://gd***.local/share/page?pt=login, log in page does not load in SSL VPN web mode.

Switch Controller

Bug ID	Description
671135	flcfg crashes while configuring FortiSwitches through FortiLink.

System

Bug ID	Description
634202	STP does not work in transparent mode.
635308	`factoryreset2` does not preserve all interfaces.
637014	FortiGate in LENC mode unable to pass firmware signature verification and shows as uncertified after GUI upgrade.
657629	ARM-based platforms do not have sensor readings included in SNMP MIBs.

Bug ID	Description
660709	The sflowd process has high CPU usage when application control is enabled.
663083	Offloaded traffic from IPsec crossing the NPU VDOM link is dropped.
663815	Low IPS HTTP throughput on SoC4 platforms.
664478	Kernel crash caused race condition on `vlif` accessing.
666205	High CPU on L2TP process caused by loop.
669951	confsyncd may crash when there is an error parsing through the internet service database, but no error is returned.
676697	When a VRF is used on SoC4 platforms, nTurbo traffic is wrongly categorized as GTPU.

User & Device

Bug ID	Description
667689	Cannot select remote certificate imported from CLI for SAML IdP.
682711	TACACS users cannot log in via console.

VM

Bug ID	Description
620654	Spoke dialup IPsec VPN does not initiate connection to hub after FG-VM HA failover in Azure.
682420	Dialup IPsec tunnel from Azure may not be re-established after HA failover.

WiFi Controller

Bug ID	Description
609549	In the CLI, the WTP profile for `radio-2` 802.11ac and 80 MHz channels does not match the syntax collection files.
680503	The current Fortinet_Wifi certificate will expire on 2021-02-11.

Known issues

The following issues have been identified in version 6.2.7. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

DNS Filter

Bug ID	Description
582374	License shows expiry date of `0000-00-00`.

Explicit Proxy

Bug ID	Description
540091	Cannot access explicit FTP proxy via VIP.
662931	Browsers change default `SameSite` cookie settings to `Lax`, and Kerberos authentication does not work in transparent proxy.
664548	When the FortiGate is configured as an explicit proxy and AV is enabled on the proxy policy, users cannot access certain FTP sites.

Firewall

Bug ID	Description
643446	Fragmented UDP traffic is silently dropped when fragments have different ECN values.
654356	Traffic is not hitting the rule it should in policy-based NGFW mode.
675353	Security policy (NGFW mode) flow-based UTM logs are still generated when policy traffic log is disabled.

FortiView

Bug ID	Description
628225	*Compromised Hosts* has error 500 when FQDN is set in `config log fortianalyzer setting`.
635309	When choosing to view *Compromised Hosts*, FortiGate returns an error 500 when FQDN is set in `config log fortianalyzer setting`.

GUI

Bug ID	Description
354464	AntiVirus archive logging enabled from the CLI will be disabled by editing the AntiVirus profile in the GUI, even if no changes are made.
514632	Inconsistent reference count when using ports in HA `session-sync-dev`.
529094	When creating an anti-spam block/allowlist entry, *Mark as Reject* should be grayed out.
535099	The SSID dialog page does not have support for the new MAC address filter.
541042	Log viewer forwarded traffic does not support multiple filters for one field.
584915	*OK* button missing from many pages when viewed in Chrome on an Android device.
584939	VPN event logs are incorrectly filtered when there are two *Action* filters and one of them contains "-".
602397	FortiSwitch port page is noticeably slow for large topology.
621254	The address group search function in GUI does not load address if there is a high amount of addresses.
623773	Security Fabric page loads slowly after adding multiple devices to FortiTelemetry.
650708	When the client browser is in a different time zone from the FortiGate, the *Guest Management* page displays an incorrect expiry time for guest users. The CLI returns the correct expiry.
655255	FortiGuard resource retrieval delay causes GUI pages to respond slowly. Affected pages include: *Firewall Policy*, *Settings* (log and system), *Explicit Proxy* (web and FTP), *System Global*, and *System CSF*.
667863	GUI does not display FortiSwitch ports when multiple FortiLink interfaces are configured.

HA

Bug ID	Description
540600	The HA `hello-holddown` value is divided by 10 in the hatalk daemon, which makes the `hello-holddown` time 10 times less than the configuration.
596551	Syncing problem after restoring one VDOM configuration.
609631	Both nodes in HA simultaneous reboot when `gtp-enhance-mode` is enabled or disabled.
652507	Sessions with `syn_ses` flags are not synced after reboot.
657376	VLAN interfaces are created on a different virtual cluster primary instead of the root primary do not sync.

Intrusion Prevention

Bug ID	Description
565747	IPS engine 5.00027 has signal 11 crash.
586544	IPS intelligent mode not working when reflect sessions are created on different physical interfaces.
587668	IPS engine 5.00035 has signal 11 crash.
590087	When IPS pcap is enabled, traffic is intermittently disrupted after disk I/O reaches IOPS limit.

IPsec VPN

Bug ID	Description
566076	IKED process signal 11 crash in an ADVPN and BGP scenario.
631804	OCVPN errors showing in logs when OCVPN is disabled.
642543	IPsec did not rekey when keylife expired after back-to-back HA failover.
644780	Rectify the consequences if password renewal on FortiClient is canceled.
650599	IKE HA sync truncates phase 2 options flags after the first eight bits.
655895	Unable to route traffic to a spoke VPN site from the hub FortiGate when the dialup IPsec VPN interface is dual stacked (IPv4/IPv6).
673049	FortiGate not sending its external interface IP in the IKE negotiation (Google Cloud Platform).

Log & Report

Bug ID	Description
606533	User observes `FGT internal error` while trying to log in or activate FortiGate Cloud from the web UI.
654363	Traffic log shows *Policy violation* for traffic hitting the allow policy in NGFW policy mode.
677540	First TCP connection to syslog server is not stable.

Proxy

Bug ID	Description
603195	Multiple WAD crashes with signal 11.
620453	Application WAD crash several times due to signal alarm.
661063	If a client sends an RST to a WAD proxy, the proxy can close the connection to the server. In this case, the relatively long session expiration (which is usually 120 seconds by default) could lead to session number spikes in some tests.
675525	No WAD sessions displayed when running `diagnose wad filter`.
680651	Memory leak when retrieving the thumbnailPhoto information from the LDAP server.

REST API

Bug ID	Description
584631	REST API admin with token unable to configure HA setting (via login session works).

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
641928	When BGP's recursive next hop can be resolved by multiple routes, the recursive distance is not taken into account when installing the routes. Multiple ECMP paths can be installed with different recursive distances to the next hop.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.
610905	SSL VPN bypassing logon count limit with different case in user name.
610995	SSL VPN web mode gets error when accessing internal website at https://st***.st***.ca/.
619296	FortiGate reverts default values of text on buttons in SSL VPN log on page.
628597	Unable to load the SSL VPN bookmark internal website, https://fi***.co.nz.
661290	https://mo***.be site is non-accessible in SSL VPN web mode.
666855	FortiOS supports verifying client certificates with RSA-PSS series of signature algorithms, which causes problems with certain clients.

Switch Controller

Bug ID	Description
588584	GUI should add support to allow using switch VLAN interface under a tenant VDOM on a managed switch VDOM.
605864	If the firewall is downgraded from 6.2.3 to 6.2.2, the FortiLink interface looses its CAPWAP setting.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
572847	The wan1, wan2, and dmz interfaces should not be configured as hardware switch members on the 60F series. The wan interface should not be configured as a hardware switch member on the 40F series.
578031	FortiManager Cloud cannot be removed once the FortiGate has trouble on contract.
591078	Get `zip conf file failed -1` error message when doing `cfg-save`.
600032	SNMP does not provide routing table for non-management VDOM.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
627629	DHCP client sent invalid DHCPREQUEST format during INIT state.

Bug ID	Description
642005	FortiGate does not send `service-account-id` to FortiManager via fgfm tunnel when FortiCloud is activated directly on the FortiGate.
643033	`get system interface transceiver port1` should return RX power and TX power for all Ch0[1-4] with a 0 value or N/A when the admin port is down on one side and the link status is down.
668856	Offloaded traffic passing through two VDOMs connected with EMAC-VLANs is sometimes dropped.

Upgrade

Bug ID	Description

658664	FortiExtender status becomes `discovered` after upgrading from 6.0.10 (build 0365).
	Workaround: change the `admin` from `discovered` to `enable` after upgrading.
	`config extender-controller extender`
	`edit <id>`
	`set admin enable`
	`next`
	`end`

User & Device

Bug ID	Description
643583	`radius-vdom-override` and `accprofile-override` do not work when administrator has 2FA enabled.

VM

Bug ID	Description
587757	FG-VM image unable to be deployed on AWS with additional HDD (st1) disk type.
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
605511	FG-VM-GCP reboots a couple of times due to kernel panic.

Bug ID	Description
608881	IPsec VPN tunnel not staying up after failing over with AWS A-P cross-AZ setup.
627106	FG-VM64 console shows `hw csum failure` for VLAN interface on mlx5_core PF.
640436	FortiGate AWS bootstrapped from configuration does not read SAML settings.
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.

WiFi Controller

Bug ID	Description
638318	FG-51E cannot authorize the FAP-C24JE.

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.