FortiOS - Release Notes

Version 6.2.9

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 14, 2022
FortiOS 6.2.9 Release Notes
01-629-721483-20220214

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-06-02	Initial release.
2021-06-09	Added 646295 to *Known issues*.
2021-06-16	Updated *Known issues*. Added FG-80D to *Special branch supported models*.
2021-06-17	Updated *FortiGate 80D boot failure* in *Special notices*. Added 721462 to *Known issues*.
2021-06-24	Added 666242 to *Known issues*.
2021-06-28	Updated *Known issues*.
2021-07-05	Updated *Known issues*.
2021-07-12	Updated *Known issues* and *Product integration and support*.
2021-07-19	Updated *Known issues*.
2021-07-26	Updated *Known issues*.
2021-08-03	Updated *Known issues*.
2021-08-09	Updated *Known issues*.
2021-08-17	Updated *Special branch supported models*.
2021-08-19	Updated *Known issues*.
2021-08-20	Updated *Resolved issues* and *Known issues*.
2021-08-25	Updated *Known issues*.
2021-08-30	Updated *Known issues*.
2021-09-07	Updated *Known issues*.
2021-09-15	Updated *Known issues*.
2021-09-20	Updated *Known issues*.
2021-09-27	Updated *Known issues*.
2021-10-04	Updated *Known issues*.
2021-10-12	Updated *Known issues*.
2021-10-19	Updated *Known issues*.
2021-11-01	Updated *Known issues*.
2021-11-15	Updated *Known issues*.

Date	Change Description
2021-11-29	Updated *Known issues*.
2021-12-13	Updated *Resolved issues* and *Known issues*.
2022-01-12	Updated *Known issues*.
2022-01-21	Updated *Known issues*.
2022-02-14	Updated *Fortinet Security Fabric upgrade* and *Product integration and support*.

Introduction and supported models

This guide provides release information for FortiOS 6.2.9 build 1234.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.9 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-80F, FG-80F-BP, FG-81E, FG-81E-POE, FG-81F, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, 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-400E-BP, 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-60F, FGR-60F-3G4G, 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-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 6.2.9. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1234.

FG-80D	is released on build 5128.
FG-200F	is released on build 7131.

FG-201F	is released on build 7131.
FG-1800F	is released on build 7197.
FG-1801F	is released on build 7197.
FG-2600F	is released on build 7197.
FG-2601F	is released on build 7197.
FG-4200F	is released on build 7197.
FG-4201F	is released on build 7197.
FG-4400F	is released on build 7197.
FG-4401F	is released on build 7197.

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`.

FortiGate 80D release

The FortiGate 80D released in 6.2.9 and later includes the removal of the LTE modem feature using the USB port on that model.

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 6.2.9 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. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC

If the Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.9. When the Security Fabric is enabled in FortiOS 6.2.9, all FortiGate devices must be running FortiOS 6.2.9.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.9 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 6.2.9 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 6.2.9 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 6.2.9 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 6.2.9, 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 6.2.9.

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 6.2.0. FortiView widgets created in previous versions are deleted in the upgrade.

Product integration and support

The following table lists FortiOS 6.2.9 product integration and support information:

Web Browsers	• Microsoft Edge 44 • Mozilla Firefox version 88 • Google Chrome version 91 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 88 • Google Chrome version 91 • 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 0297 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	• 4.0.0 and later. For compatibility with latest features, use latest 4.0 version.
AV Engine	• 6.00161
IPS Engine	• 5.00239
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

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 88 Google Chrome version 91
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 88 Google Chrome version 91
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 88
macOS Big Sur 11.0	Apple Safari version 14 Mozilla Firefox version 88 Google Chrome version 91
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 6.2.9. For inquires about a particular bug, please contact Customer Service & Support.

IPsec VPN

Bug ID	Description
720024	Signature authentication IKE negotiation gets stuck and tunnel is not set up. This issue appears after a reboot, and can become unstuck by running `get vpn ike gateway`.

Proxy

Bug ID	Description
717157	When using certificate inspection in a firewall policy, the WAD daemon might crash when clients try to connect to a web proxy server through the FortiGate in transparent mode or through a web proxy forward server.

SSL VPN

Bug ID	Description
714604	SSL VPN daemon may crash when connection releases.

System

Bug ID	Description
695803	Unable to reorder firewall DoS policy in GUI or CLI.
735492	Many processes are in a "D" state due to `unregister_netdevice`.

Upgrade

Bug ID	Description
716912	SSH access may be lost in some cases after upgrading to 6.2.8, 6.4.6, or 7.0.0.

Known issues

The following issues have been identified in version 6.2.9. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
665173	Crash logs are sometimes truncated/incomplete.

DNS Filter

Bug ID	Description
582374	License shows expiry date of `0000-00-00`.
682060	DNS proxy is holding 60% memory caused by retransmitted DNS messages sent from DNS clients, which causes the FortiGate to enter conserve mode.

Explicit Proxy

Bug ID	Description
540091	Cannot access explicit FTP proxy via VIP.
654455	Proxy policy destination address set to none allows all traffic.
681969	FSSO explicit proxy authentication appears as basic instead of FSSO.

Firewall

Bug ID	Description
561170	Traffic is blocked by NGFW policy when SDN connector firewall address is configured in policy.

Bug ID	Description
644225	Challenge ACK is being dropped.
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed. **Workaround**: clear the session after policy change.
716317	IPS user quarantine ban event is marking the sessions as dirty.
719925	Load balancing is not allowed with a flow-based policy, even if the server type is configured as IP or TCP.
730803	Applying a traffic shaping profile and outbound bandwidth above 200000 blocks the traffic.

FortiView

Bug ID	Description
635309	When FortiAnalyzer logging is configured using an FQDN domain, the GUI displays a 500 error message on the FortiView *Compromised Hosts* page.
673225	FortiView *Top Traffic Shaping* widget does not show data for outbound traffic if the source interface's role is WAN. Data is displayed if the source interface's role is LAN, DMZ, or undefined.

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 antispam 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 "-".
602102	Warning message is not displayed when a user configures an interface with a static IP address that is already in use.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.

Bug ID	Description
610572	Guest user credentials never expire if a guest user logs in via the WiFi portal while an administrator is actively viewing the user's account via the GUI. If the administrator clicks *OK* in the user edit dialog after the guest user has logged in, the user's current login session is not subject to the configured expiration time. **Workaround**: click *Cancel* instead of *OK* to close the dialog.
621254	When creating or editing an IPv4 policy or address group, firewall address searching does not work if there is an empty wildcard address due to a configuration error.
664007	GUI incorrectly displays the warning, *Botnet package update unavailable, AntiVirus subscription not found.*, when the antivirus entitlement is expiring within 30 days. The actual botnet package update still works within the active entitlement duration.
672599	After performing a search on firewall *Addresses*, the matched count over total count displayed for each address type shows an incorrect total count number. The search functionality still works correctly.
674592	When config `ha-mgmt-interfaces` is configured, the GUI incorrectly shows an error when setting overlapping IP address.
682440	On *Firewall Policy* list, the tooltip for *IP Pool* incorrectly shows *Port Block Allocation* as being exhausted if there are expiring PBAs available to be reallocated.
688994	The *Edit Web Filter Profile* page incorrectly shows that a URL filter is configured (even though it is not) if the URL filter entry has the same name as the web filter profile in the CLI.
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI *Forward Traffic* log page can take time to load if there is no specific filter for the time range. **Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs.
720613	The event log sometimes contains duplicated lines when downloaded from the GUI.
722832	When LDAP server settings involve FQDN, LDAPS, and an enabled server identity check, the following LDAP related GUI items do not work: LDAP setting dialog, LDAP credentials test, and LDAP browser.

HA

Bug ID	Description
669301	When sending UDP packets, hasync code uses the wrong buffer size so that it may overwrite beyond the buffer to other corrupted memory.
693178	Sessions timeout after traffic failover goes back and forth on a transparent FGSP cluster.
695067	When there are more than two members in a HA cluster and the HA interface is used for the heartbeat interface, some RX packet drops are observed on the HA interface. However, no apparent impact is observed on the cluster operation. **Workaround**: do not use the HA interface as a heartbeat interface.

Bug ID	Description
709518	Secondary device is unable to connect to FortiCloud with secondary IP as the source IP.
710236	Heartbeat interfaces do not get updated under `diagnose sys ha dump-by <group |memory>` after HA `hbdev` configuration changes.
715939	Cluster is unstable when running interface configuration scripts. For example, when inserting many VLANs, hatalk will get a lot of `intf_vd_changed` events and recheck the MAC every time, which blocks hatalk from sending heartbeat packets for a long time and the peer loses it.
722284	When there is a large number of VLAN interfaces (around 600), the FortiGate reports `VLAN heartbeat lost on subinterface vlan` error for multiple VLANs.
723130	`diagnose sys ha reset-uptime` on the secondary devices triggers a failover on a cluster with more than two members.
744826	API key (token) on the secondary device is not synchronized to the primary when `standalone-config-sync` is enabled.
746008	DNS may not resolve on the correct blade in a 6K/7K virtual cluster environment.

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.
680501	Destination interfaces are set to unknown for previous ADVPN shortcuts sessions.
689259	Flow-based AV scanning does not send specific extension files to FortiSandbox.
693800	IPS memory spike on 6.2.7 running version: 5.00229.
721462	Memory usage increases up to conserve mode after upgrading IPS engine to 5.00239.

IPsec VPN

Bug ID	Description
578879, 676728	IPsec tunnel bandwidth usage is not correct on the GUI widget and SNMP graph when NPU is doing host offloading.
714400	Dynamic IKEv2 IPsec VPN fails to establish after adding new phase 2 with mismatched traffic selector.

Bug ID	Description
717082	FortiGate keeps initiating DHCP SA rekey after lifetime expires.
752947	The hub sometimes allows the IKEv2 IPsec tunnel with a spoke to be established that uses an expired or revoked certificate.

Log & Report

Bug ID	Description
606533	User observes `FGT internal error` while trying to log in or activate FortiGate Cloud from the web UI.
703738	Log upload through user proxy is randomly terminated.
713014	Cannot perform disk scan after enabling disk raid.
722315	System might generate garbage administrator log events upon session timeout.
724827	Syslogd is using the wrong source IP when configured with `interface-select-method auto`.

Proxy

Bug ID	Description
520176	Multiple WAD crashes observed with signal 6. The issue could be reproduced with a slow server that will not respond the connection in 10 seconds, and if the configuration changes during the 10 seconds.
568905	WAD crashes due to RCX having a null value.
582464	WAD SSL crash due to wrong cipher options chosen.
586281	WAD memory corruption.
615391	Reusing the buffer region causes frequent WAD crashes.
663088	Application control in Azure fails to detect and block SSH traffic with proxy inspection.
670339	Proxy-based SSL out-band-probe session has local out connection. Since the local out session will not learn the router policy, it makes all outbound connections fail if there is no static router to the destination.
675343	WAD crashes with transparent web proxy when connecting to a forward server.
691468	WAD IPS crashes because task is scheduled after closing.
714109	YouTube server added new URLs (`youtubei/v1/player, youtubei/v1/navigator`) that caused proxy option to restrict YouTube access to not work.

Bug ID	Description
719681	Flow control failure occurred while transferring large files when `stream-scan` was running, which sometimes resulted in WAD memory spike.
726999	WAD crash on `wad_hash_map_del`.
727349	Traffic is stuck if HTTP POST does not have an end of boundary.
733760	Proxy inspection firewall policy with proxy AV blocks POP3 traffic of the Windows 10 built-in Mail app.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.

REST API

Bug ID	Description
584631	REST API admin with token unable to configure HA setting (via login session works).
663441	REST API unable to change status of interface when VDOMs are enabled.
713445	For API user tokens with CORS enabled and set to wildcard *, direct API requests using this token are not processed properly. This issue impacts FortiOS version 5.6.1 and later. **Workaround**: set CORS to an explicit domain.
714075	When CORS is enabled for REST API administrators, POST and PUT requests with body data do not work with CORS due to the pre-flight requests being handled incorrectly. This only impacts newer browser versions that use pre-flight requests.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
611708	Make SNMP get BGP peer state timely once BGP neighbor enters or exits established state.
655447	BGP prefix lifetime resets every 60 seconds when scanning BGP RIB.
661270	OSPF is stuck in loading state when there is a large amount of OSPF interfaces.
662655	The OSPF neighborship cannot be established; get MD5 authentication error when the wrong MD5 key is deleted after modifying the key.
693396	hasync daemon was busy in dead loop if FD resource was used up when flushing routes from the kernel.

Bug ID	Description
693496	SD-WAN rules not working for FortiAnalyzer settings because the `interface-select-method` is implemented on a remote device FortiAnalyzer/FDS but not added to FortiView/log viewing API.
697658	FortiCloud activation does not honor the `set interface-select-method` command under `config system fortiguard`.
723726	BGP session drops between virtual wire pair with `auto-asic-offload` enabled in policy.
725322	Improve the help text for `distance` to indicate that 255 means unreachable.
748733	Remote IP route shows `incomplete inactive` in the routing table, which causes issues with BGP routes where the peer is the next hop.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
635183	ACI dynamic address cannot be retrieved in HA vcluster2 from SDN connector.
666242	Automation stitch CLI scripts fail with greater than 255 characters; up to 1023 characters should be supported.
735717	vmwd gives an error when folders are created in the vSphere web interface, and vmwd ignores the IP addresses from vApp.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.
646295	When DNS domain is configured, requests with NTLM of hostname only bookmark could not get response from server.
677057	SSL VPN firewall policy creation via CLI does not require setting user identity.
677548	In SSL VPN web mode, options pages are not shown after clicking the option tag on the left side of the webpage on an OWA server.
677668	sslvpnd crashes due to wrong application index referencing the wrong shared memory when daemons are busy. Crash found when RADIUS user uses Framed-IP.
695404	WALLIX personal bookmark issue in SSL VPN portal.

Bug ID	Description
695763	FortiClient iOS 6.4.5. has new feature that allows bypassing of 2FA for SSL VPN 2FA. The FortiGate should allow access when 2FA is skipped on FortiClient.
697637	FortiToken Cloud user not working when in a user group.
706646	SolarWinds Orion NPM platform's web application has issues in SSL VPN web mode.
715928	SSL VPN signal 11 crashes at `sslvpn_ppp_associate_fd_to_ipaddr`. For RADIUS users with Framed-IP using tunnel mode, the first user logs in successfully, then a second user with the same user name logs in and kicks the first user out. SSL VPN starts a five-second timer to wait for the first user resource to clean up. However, before the timer times out, the PPP tunnel setup fails and the PPP context is released. When the five-second timer times out, SSL VPN still tries to use the PPP context that has already been released and causes the crash.
718170	SSL VPN web portal does not show thumbnails of videos for an internal JS-based web server.
726576	Internal webpage with JavaScript is not loading in SSL VPN web mode.
731278	Customer internal website (ac***.sa***.com) does not load properly when connecting via SSL VPN web mode.
745499	In cases where a user is establishing two tunnel connections, there is a chance that the second session knocks out the first session before it is updated, which causes a session leak.

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 loses its CAPWAP setting.
689403	Unable to add FSW-448E using serial number on FortiGate.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
578031	FortiManager Cloud cannot be removed once the FortiGate has trouble with contract.
595244	There is duplicate information when checking interface references in global.
600032	SNMP does not provide routing table for non-management VDOM.

Bug ID	Description
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
627236	TCP traffic disruption when traffic shaper takes effect with NP offloading enabled.
627645	When upgrading FG-100D, several processes randomly go into D state, which generates cluster and service issues.
641708	FTLF8536P4BCV shows `This transceiver is not certified by Fortinet`, corrupt part number and serial number after HA cluster sync.
648014	FortiDDNS is unable to update the renewed public IP address to FortiGuard server in some error conditions.
675418	FortiManager CLI script for 2FA FortiToken mobile push does not trigger activation code email.
681791	Install preview does not show all changes performed on the FortiGate.
682227	DSL creates a default route to 240.0.0.1 after changing any configuration on a DSL interface.
687519	Bulk changes through the CLI are very slow with 24000 existing policies.
689317, 698927	After pushing the interface configuration from FortiManager, the device index is incorrectly set to 0.
691729	WWAN interface on FG-40F- 3G4G eventually goes offline until a reboot or configuration change occurs.
692490	When an `<entry name>` is on the same line as `config <setting> <setting> <entry name>`, it is not handled properly to send to FortiManager.
694202	`stpforward` does not work with LAG interfaces on a transparent VDOM.
696556	Support `gtp-enhance-mode` (GTP-U) on FG-3815D.
699902	SNMP query of fgFwPolTables (1.3.6.1.4.1.123456.101.5.1.2.1) causes high CPU on a specific configuration.
702135	cmdbsvr memory leak due to unreleased memory allocated by OpenSSL.
702932	FG-1500D reboots suddenly after COMLog reported kernel panic and voipd is tainted.
702966	There was a memory leak in the administrator login debug that caused the getty daemon to be killed.
704981	LLDP transmission fails if there are nested software switches.
713324	Command fail when running `execute private-encryption-key <xxx>`.
714805	FortiManager shows auto update for down port from FortiGate, but FortiGate event logs do not show any down port events when user shuts down the `ha monitor dev`.
715978	NTurbo does not work with EMAC VLAN interface.
721733	IPv6 networks are not reachable shortly after FortiGate failover because an unsolicited neighbor advertisement is sent without a router flag.
722273	SA is freed while its timer is still pending, which leads to a kernel crash.
740649	FortiGate sends CSR configuration without double quote (") to FortiManager.

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`

685705	After upgrading to 6.2.6, get errors `No such file or directory` and `No space left on device` on FWF-50 and FWF-51E.

User & Device

Bug ID	Description
595583	Device identification via LLDP on an aggregate interface does not work.
688989	Two-factor authentication can be bypassed with some configurations.

701356	When a GUI administrator certificate, `admin-server-cert`, is provisioned via SCEP, the FortiGate does not automatically offer the newly updated certificate to HTTPS clients. FortiOS 7.0.0 and later does not have this issue.
	Workaround: manually unset `admin-server-cert` and set it back to the same certificate.
	`config system global`
	`unset admin-server-cert`
	`end`
	`config system global`
	`set admin-server-cert <scep_certificate>`
	`end`

710212	RADIUS accounting port is occasionally missing.
725056	FSSO local poller fails after recent Microsoft Windows update (KB5003646, KB5003638, ...).
750551	DST_Root_CA_X3 certificate is expired. **Workaround**: see the Fortinet PSIRT blog, https://www.fortinet.com/blog/psirt-blogs/fortinet-and-expiring-lets-encrypt-certificates, for more information.

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.
608881	IPsec VPN tunnel not staying up after failing over with AWS A-P cross-AZ setup.
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.
685782	HTTPS administrative interface responds over heartbeat port on Azure FortiGate despite `allowaccess` settings.

Web Filter

Bug ID	Description
672994	Web filter warning message does not contain certification chain.
717619	Running a remote CLI script from FortiManager can create a duplicated FortiGuard web filter category.
739349	Web filter local rating configuration check might strip the URL, and the URL filter daemon does not start when `utm-status` is disabled.

WiFi Controller

Bug ID	Description
676689	RADIUS traffic not matching SD-WAN rule when using wpad daemon for wireless connection.
709871	After the firmware upgrade, the AP cannot register to the central WLC because NPU offload changed the source and destination ports from 4500 to 0.
739793	VM license file generated by FortiCare lacks new line at the end and causes cw_acd process to constantly restart. **Workaround**: import a certificate called cw_ac_cert or ask Fortinet customer support to regenerate the VM license file.

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.