FortiOS - Release Notes

Version 6.2.6

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

FORTINET TRAINING 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

May 23, 2023
FortiOS 6.2.6 Release Notes
01-626-661160-20230523

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-11-12	Initial release.
2020-11-17	Updated *New features or enhancements* and *Known issues*. Added *SSL traffic over TLS 1.0 will not be checked and will be bypassed by default* to *Special notices*. Added FG-80F, FG-80F-BP, FG-81F, FG-100F, and FG-101F to *Special branch supported models*.
2020-11-23	Added 660165 to *Changes in CLI defaults*. Updated *Known issues* and *Resolved issues*.
2020-11-25	Updated *Changes in table size*, *Known issues*, and *Resolved issues*.
2020-12-02	Added FGR-60F and FGR-60F-3G4G to *Special branch supported models*.
2020-12-15	Updated *Known issues* and *Resolved issues*.
2020-12-30	Added FG-80D to *Supported models*.
2021-02-05	Updated *Known issues* and *Resolved issues*.
2021-02-12	Updated *Known issues*.
2021-02-16	Added FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F to *Special branch supported models*. Updated *Known issues.*
2021-02-17	Updated *Resolved issues*.
2021-02-24	Updated *Known issues*.
2021-03-08	Updated *Known issues* and *Built-in IPS engine*.
2021-04-19	Added FWF-80F-2R to *Special branch supported models*.
2021-05-03	Updated *Known issues*.
2021-05-18	Updated *Known issues*.
2021-05-31	Updated *Known issues* and *Resolved issues*.
2021-06-16	Updated *Known issues*.
2021-07-12	Updated *Known issues*.
2021-07-19	Added FWF-81F-2R to *Special branch supported models*.
2021-07-26	Updated *Known issues*.
2021-08-09	Updated *Known issues*. Added FWF-81F-2R-POE to *Special branch supported models*.

Date	Change Description
2021-08-20	Added FG-80F-POE and FG-81F-POE to *Special branch supported models*.
2021-08-23	Updated *Known issues*.
2021-09-07	Updated *Resolved issues*.
2021-10-07	Updated *Known issues*.
2022-01-04	Added FWF-80F-2R-3G4G-DSL, FWF-81F-2R-3G4G-DSL, and FWF-81F-2R-3G4G-POE to *Special branch supported models*.
2023-05-23	Updated *SSL traffic over TLS 1.0 will not be checked and will be bypassed by default*.

Introduction and supported models

This guide provides release information for FortiOS 6.2.6 build 1175.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.6 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-80D, 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 6.2.6. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1175.

FG-80F	is released on build 5909.
FG-80F-BP	is released on build 5909.
FG-80F-POE	is released on build 7176.

FG-81F	is released on build 5909.
FG-81F-POE	is released on build 7176.
FG-100F	is released on build 5911.
FG-101F	is released on build 5911.
FG-1800F	is released on build 6988.
FG-1801F	is released on build 6988.
FG-2600F	is released on build 6988.
FG-2601F	is released on build 6988.
FG-4200F	is released on build 6988.
FG-4201F	is released on build 6988.
FG-4400F	is released on build 6988.
FG-4401F	is released on build 6988.
FGR-60F	is released on build 5930.
FGR-60F-3G4G	is released on build 5930.
FWF-80F-2R	is released on build 7032.
FWF-80F-2R-3G4G-DSL	is released on build 7219.
FWF-81F-2R	is released on build 7134.
FWF-81F-2R-POE	is released on build 7134.
FWF-81F-2R-3G4G-DSL	is released on build 7219.
FWF-81F-2R-3G4G-POE	is released on build 7162.

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`, set the following to `block` in the SSL protocol settings:
  - in FortiOS 6.2.6 and later:

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl block
        end
    next
end
```

  - in FortiOS 6.4.3 and later:

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl-negotiation block
        end
    next
end
```

New features or enhancements

Bug ID	Description

641524	Add interface selection for IPS TLS protocol active probing.
	`config ips global`
	`  config tls-active-probe`
	`  set interface-selection-method {auto | sdwan | specify}`
	`  set interface <interface>`
	`  set vdom <VDOM>`
	`  set source-ip <IPv4 address>`
	`  set source-ip6 <IPv6 address>`
	`  end`
	`end`

652003	In a tenant VDOM, allow `lldp-profile` and `lldp-status` to be configurable on a leased switch port.

657598	In an application control list, the `exclusion` option allows users to specify a list of applications that they wish to exclude from an entry filtered by category, technology, or others.
	`config application list`
	`  edit <list>`
	`  config entries`
	`  edit 1`
	`  set category <ID>`
	`  set exclusion <signature ID> ... <signature ID>`
	`  next`
	`  end`
	`  next`
	`end`

660295	Provide specific SNMP objects (OIDs) that allow the status of the mobile network connection to be monitored.

Changes in CLI defaults

Bug ID	Description

660165	Rename `members` to `priority-members` under manual mode SD-WAN service.
	`config system virtual-wan-link`
	`  config service`
	`  edit 2`
	`  set mode manual`
	`  set priority-members 2 3`
	`  next`
	`  end`
	`end`

Changes in table size

Bug ID	Description
609785	Changed the `switch-controller.managed-switch` scale numbers for FG-1100E/1101E platform from 128 to 196.
626765	FG-60F/61F and FWF-60F/61F total WTP size is increased to 64.

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 6.2.6 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 6.2.6. When the Security Fabric is enabled in FortiOS 6.2.6, all FortiGate devices must be running FortiOS 6.2.6.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.6 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 6.2.6 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 6.2.6 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 6.2.6 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 6.2.6, 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 6.2.6.

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, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *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 6.2.6 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 17. 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 17. 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 17 and Fortinet Security Fabric upgrade on page 17. 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 0294 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 6.2.6. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
560044	Secondary device blades occasionally report critical log event `Scanunit initiated a virus engine/definitions update`. Affected models: FG-5K, 6K, and 7K series.

Data Leak Prevention

Bug ID	Description
616918	DLP cannot detect attached ZIP and PDF files when receiving emails via MAPI over HTTPS.

DNS Filter

Bug ID	Description
649985	Random SDNS rating timeout events on 6K/7K SLBC with FGSP.

Endpoint Control

Bug ID	Description
637454	Cloud-based EMS FSSO connector in FortiGate failed to connected with FortiClient EMS proxy in public cloud.

Explicit Proxy

Bug ID	Description
599637	Web proxy does not work properly to redirect Chrome browser to websites when disclaimer is enabled in proxy policy.
617934	FortiGate web proxy should support forward server on TLS 1.3 certificate inspection connection.
630434	WAD crashed at wad_ssl_port_p2s_supported_versions with signal 11.
634515	HTTP 1.1 host header is lost in FortiGuard web proxy requests.
644121	Explicit proxy error 504, DNS fails for a specific domain.

Firewall

Bug ID	Description
586764	Abnormal prolonged CPU spike with cmdbsvr and WAD processes when making change to large policy list (10 000+ policies).
586995	Cluster VDOM policy statistics data is not correct when VFID is different for same VDOM on primary/secondary.
595949	Any changes to the security policy table causes the hit count to reset.
628841	Internet service entry not detected due to some IP ranges being duplicated.
633856	Sessions are marked as dirty when a route change happens, but the route still exists.
644638	Policy with Tor-Exit.Node as source is not blocking traffic coming from Tor.
644865	Query string parameters omitted (HTTP redirect, SSL offloading).
647410	`append` command allows mixing VIP and firewall address as destination objects in a firewall policy.
648951	External threat feed entry `0.0.0.0/0` shows as invalid but it blocks traffic.
653828	When web filter and application control are configured, blocked sessions to play.google.com remain in the session table for 3600 seconds.
660461	Configuration changes take a long time, and ipsmonitor and cmdbsrv processes go up to 100% of CPU in a large, complex configuration.

FortiView

Bug ID	Description
643198	*Threats* drilldown for *Sources*, *Destinations*, and *Country/Region* (1 hour, 24 hours, 7 days) gives the error, *Failed to retrieve FortiView data*.
660753	In FortiView *Sources* dashboard, after filtering by subnet, drilling down will always show the first entry.

GUI

Bug ID	Description
598222	After upgrading to 6.4.x from 6.2.5 and earlier, users must clear the browser cache for the best user experience with the new firmware.
612236	RADIUS test fails from the GUI as it does not use the configured *Authentication method*, and authentication fails; test passes on the CLI.
638752	FortiGates in an HA A-P configuration may lose GUI access to the HA secondary device after a period of 8 days of inactivity, when at least one static IPv6 address is configured on an interface.
650307	GUI does not show the configured external FortiGuard category in the SSL-SSH profile's exempt list.
651711	Unable to select an address group when configuring *Source IP Pools* for an SSL VPN portal.
653726	Filtering log results with a regular expression incorrectly yields no results.
660165	When creating SD-WAN rules in the GUI, the destination interface preference is not saved when the strategy is manual.
663351	Connectivity test for RADIUS server using CHAP authentication always returns failure.
666545	When in HA mode, the FortiGate GUI may take a long time or may fail to show traffic logs from FortiAnalyzer. Log retrieval from disk does not have this issue.

HA

Bug ID	Description
615001	LAG does not come up after link failed signal is triggered.
626715	Out-of-sync issue caused by firewall address group member is either duplicated or out of order.
630070	HA is failing over due to cmdbsvr crashes.

Bug ID	Description
634604	SCTP sessions are not fully synchronized between primary and secondary devices in version 5.6.11 on FG-3240C.
637711	CSR on cluster primary is generating out-of-sync alerts on secondary and tertiary units.
639307	Both primary and secondary consoles keep printing `get_ha_sync_obj_sig_4dir: stat /etc/cert/ca/5c44d531.0 error 2`.
640428	SSL VPN related auth login user event logs do not require HA to be in sync.
643958	Inconsistent data from FFDB caused several confsyncd crashes.
647679	Inconsistent values for HA cluster inside the SNMP.
648073	HA cluster uses physical port MAC address at the time of HA failover.
651674	Long sessions lost on new primary after HA failover.
654341	The new join-in secondary chassis failed to sync, while primary chassis has 6K policies in one VDOM.

Intrusion Prevention

Bug ID	Description
655371	Logging is intermittent for FortiGate IDS passive in one-armed sniffer mode.

IPsec VPN

Bug ID	Description
592361	Cannot pass traffic over ADVPN if: `tunnel-search` is set to `nexthop`, `net-device disable`, `mode-cfg enable`, and `add-route disable`.
611451	ADVPN spoke one behind NAT shortcut cannot connect to another spoke that is not behind NAT.
639806	User name log empty when IPsec dialup IKEv2 has client RSA certificate with empty subject.
646012	DHCP over IPsec randomly works when `net-device` is disabled.
647285	IKE HA sync IPsec SA fails on receiver when ESP null crypto algorithm is used.
655739	`local-gw` is replaced with primary IP on a secondary device when the secondary IP is used as a `local-gw`.
659535	Setting same `phase1-interface` in SD-WAN member and SD-WAN zone causes iked watchdog timeout.

Log & Report

Bug ID	Description
555161	Application miglogd crashes when numerous DLP logs are generated, where DLP archive files use up system inodes.
583499	Improve local log search logic from aggressive to passive mode to save resources and CPU.
634947	rlogd signal 11 crashes.
641450	The miglogd processes is bound to busy CPUs, even though there are other completely idle CPUs available.
647741	On FG-60F, logging and FortiCloud reporting incorrect IPv6 bandwidth usage for sessions with NPU offload.
650325	The miglogd process crashes with signal 11 (segmentation fault).

Proxy

Bug ID	Description
550350	Should not be able to set `inspection-mode proxy` with IPS-enabled only policy.
578850	Application WAD crash several times due to signal alarm.
582475	WAD is crashing with signal 6 in `wad_fmem_free` when processing SMB2/CIFS.
608387	WAD virtual server with HTTP multiplexing enabled causes crash after server is detached because the HTTP server object is detached from the HTTP session.
617322	DLP FTP proxy with splice option sends delete command to server before data transfer completes.
619707	When Kerberos (negotiate without NTLM) authentication method is used for web proxy user authentication, there may be a rare memory leak issue. This memory leak issue may eventually cause the FortiGate to go into conserve mode once it occurs after many users are authenticated by Kerberos repeatedly over time.
620453	Application WAD crash several times due to signal alarm.
621787	On some smaller models, WAD watchdog times out when there is a lot of SSL traffic.
629504	SSH status in SSL profile changes to `deep-inspection` from `disable` after upgrading.
638039	Delete validation is not working for *Protecting SSL Server* profile.
647923	WAD has multiple signal 11 crashes at `wad_ssl_cert_get_auth_status`.
648831	WAD memory leak caused by Kerberos proxy authentication.
653099	Wildcard URL filter in proxy mode with `?` and `*` not always handled properly.

Bug ID	Description
656830	FortiGate should be in SSL bypass mode for TLS 1.2 certificate inspection with client certificate request.
658654	Cannot access specific website using proxy-based UTM with certification inspection due to delays from the server in replying to ClientHello message when a second connection from the same IP is also waiting for ClientHello.
666522, 666686	Proxy mode is blocking web browsing for some websites due to certificate inspection.

Routing

Bug ID	Description
624621	Log traffic to remote servers does not follow SD-WAN rules.
627901	`set dscp-forward` option is missing when using maximize bandwidth strategy in SD-WAN rule.
632285	Health check SLA status log shows configured bandwidth value instead of used bandwidth value.
641022	Kernel does not remove duplicate routes generated by SD-WAN health checks when hostname IP changes.
641050	Need support for SSL VPN web mode traffic to follow SD-WAN rules/policy route.
646418	SD-WAN information available in session list is confusing.
654482	SD-WAN route tag is removed with multiple BGP paths in place.
662845	HA secondary also sends SD-WAN `sla-fail-log-period` to FortiAnalyzer.
666829	Application bfdd process crashes.

Security Fabric

Bug ID	Description
619696	Automation stitch traffic is sent via `mgmt` with `ha-direct` to AWS Lambda after upgrading from 6.0.9 to 6.2.3.
629723	SDN dynamic address import is too slow, and HA sync may miss endpoints in high scale and stress conditions.

SSL VPN

Bug ID	Description
548599	SSL VPN crashes on parsing some special URLs.
573853	TX packet drops on SSL root interface.
611498	SMB/CIFS traffic via SSL VPN web mode not using correct SNAT IP (IP pool).
620793	A page inside a bookmark not opening in SSL VPN web mode.
624288	After SSL VPN proxy, one JS file of http://www.cm***-rm***.ca runs with an error.
627456	Traffic cannot pass when SAML user logs in to SSL VPN portal with group match.
630432	Slides on https://re***.nz website are displayed in SSL VPN web mode.
631082	FortiManager tabs/page do not load when accessed via SSL VPN web mode.
634210	SSL VPN daemon crash due to `limit-user-login`.
635814	FortiGate GUI cannot be rendered and displayed via SSL VPN portal.
636332	With SSL VPN proxy JIRA web application, get one wrong URL without proxy path.
639431	Three of the internal applications/portal bookmarks do not load/partially work with SSL VPN web mode.
641379	Internal SharePoint 2019 website cannot be accessed in SSL VPN web portal.
643749	SSL VPN crashes when accessing a realm with an incorrect user, or when the correct user enters the wrong password.
644506	Cannot authenticate to SSL VPN using 2FA if remote LDAP user and user within RADIUS group has same user name and password.
645368	FortiClient randomly fails to connect to SSL VPN tunnel mode stuck at 98% with two-factor authentication token.
648192	DTLS tunnel performance improvements by allowing multiple packets to be read from the kernel driver, and redistributing the UDP packets to several worker processes in the kernel.
648433	Internal website loading issue in SSL VPN web portal for ca***.fr.
649130	SSL VPN log entries display users from other VDOMs.
652880	SSL VPN crashes in a scenario where a large number of groups is sent to fnbam for authentication.
657689	The system allows enabling split tunnel when the SSL VPN policy is configured with destination `all`. It is not consistent with 5.6.x and 6.0.x.
663532	Get `no more IP address available` error when users connect to SSL VPN after upgrading to 6.2.5.
665879	When SSL VPN processes the HTTP/HTTPS response with content disposition, it will change the response body since the content type is HTML.

Switch Controller

Bug ID	Description
649913	HA cluster not synchronizing when configuring an active LACP with MCLAG via FortiManager.
652745	Compatibility issues with FortiGate in 6.0 branch and FortiSwitch 424E-Fiber.

System

Bug ID	Description
574716	The ospfNbrState OID takes too long to update.
582536	Link monitor behavior is different between FGCP and SLBC clusters.
583472	When system is in an extremely high memory usage state (~90%), a power supply status `Power supply 1 AC is lost` might be mistakenly logged.
585882	Error in log, `msg="Interface 12345678001-ext:64 not found in the list!"`, while creating a long name VDOM in FG-SVM.
594264	NP-offloaded active TCP/UDP sessions established over IPsec VPN tunnels will timeout at session TTL expiry.
594931	FG-60F/61F memory usage causes conserve mode by enabling/disabling UTM.
597893	FortiExtender interface admin status changes cannot be detected by FortiManager because the FortiGate checksum does not change.
598464	Rebooting FG-1500D in 5.6.x during upgrade causes an L2 loop on the heartbeat interface and VLAN is disabled on the switch side.
598928	FortiGate restarts FGFM tunnel every two minutes when FortiManager is defined as FQDN.
602643	Interface gets removed from SD-WAN after rebooting when the interface is defined in both SD-WAN and zone.
605723	FG-600E stops sending out packets on its SPF and copper port on NP6.
606360	HQIP loopback test failed with configured software switch.
607754	FortiGuard push update is not working properly from override (FortiManager)
609112	IPv6 push update fails.
609783	SNMP failed to retrieve HA cluster secondary information from secondary serial number in TP mode.
619023	Proxy ARP configuration not loaded after interface shut/not shut.
627269	Wildcard FQDN not resolved on the secondary unit.

Bug ID	Description
628642	Issue when packets from same session are forwarded to each LACP member when NPx offload is enabled.
630146	FG-100F memory configuration check.
630861	Support FortiManager when `private-data-encryption` is enabled in FortiOS.
631296	Forward or local bi-directional traffic from NPU inter-VDOM links through separate VDOMs is subject to high latency.
631689	FG-100F cannot forward fragmented packets between hardware switch ports.
633298	10G ports x1/x2 cannot be set as interfaces in firewall `acl/acl6` policies.
633827	Errors during fuzzy tests on FG-1500D.
634929	NP6 SSE drops after a couple of hours in a stability test.
636999	LTE does not connect after upgrading from 6.2.3 on FG-30E-3G4G models.
637983	FG-100F memory configuration check fails because of wrong threshold.
641419	FG-40F LAN interfaces are down after upgrading to 6.2.4 (build 5632).
642327	FortiGate unable to boot with kernel panic by cmdbsvr when VLAN is configured on redundant interface with non-NPU port.
643188	Interface `forward-error-correction` setting not honored after reboot.
644380	FG-40F/60F kernel panic if upgrading from 6.4.0 due to configuration file having a name conflict of `fortilink` as both aggregate interface and virtual switch name.
644427	Interface `forward-error-correction` setting not honored after reboot. Affected platforms: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3400E, and FG-3600E.
645363	SNMP monitoring does not provide the SD-WAN member interface name.
645848	FortiOS is providing self-signed CA certificate intermittently with flow-based SSL certificate inspection.
647151	Unable to configure aggregate interface type on FG-30E-3G4G.
647593	After reboot, `forward-error-correction` value is not maintained as it should be.
647777	FortiGate not responding to DHCP relay requests from clients behind a DHCP relay.
654159	NP6Xlite traffic not sent over the tunnel when NPU is enabled.
658933	Under some circumstances, it was possible for Update D to create zombie processes.
661503	Existing ffdb_map_res package was not automatically removed after upgrading on small storage FortiGates, even though their creation was removed in 6.2.4.
662681	Policy package push from FortiManager fails the first time, and succeeds the second time if it is blank or has no changes.
662989	FG-40F/41F aggregate interface gets removed after upgrading to 6.2.5 from 6.2.4 firmware version.

Bug ID	Description
663603	The maximum number of IPS supported by each NTurbo load balancer should be 7 instead of 8 on FG-3300E and FG-3301E.
665000	HA LED off issue on FG-1100E/1101E models in 6.0.x.
666030	Empty firewall objects after pushing several policy deletes.
670838	It takes a long time to set the member of a firewall address group when the member size is large. In the GUI, cmdbsvr memory usage goes to 100%. In the CLI, newcli memory usage goes to 100%.
677825	Traffic on VLAN and NPU VDOM link interfaces fails after switching from standalone to HA mode.
678852	Support EoIP acceleration with NP7 platforms.
689345	npd crashes because FOS object is null.
689619	Traffic dropped with NP7 IPsec hardware acceleration when packet size higher than PMTU and lower than tunnel MTU.
689625	Kernel crashes when using FCLF8522P2BTLFTN SFPs on HA interfaces. Affected models: FG-1800F and FG-1801F.
689735	NP7 drops frames shorter than 32 bytes at HTX. HA session synchronization packets are not balanced to multiple HRX queues because the frames have the same source and destination MAC address.

Upgrade

Bug ID	Description
656869	FG-100F/101F may continuously boot upon upgrading from FortiOS 6.4.0. **Workaround**: back up the 6.4.0 configuration, perform a clean install via TFTP of FortiOS 6.4.2, and restore the 6.4.0 configuration.
662452	SSH status in `ssl-ssh-profile` changes to `deep-inspection` from `disable` after upgrade.

User & Device

Bug ID	Description
546794	De-authentication of RSSO user does not clear the login from the motherboard.
580155	fnbamd crash.
591461	FortiGate does not send user IP to TACACS server during authentication.
620097	Persistent sessions for de-authenticated users.

Bug ID	Description
659456	REST API authentication fails for API user with PKI group enabled due to fnbamd crash.
663399	`interface-select-method` not working for RADIUS configuration.

VM

Bug ID	Description
587180	FG-VM64-KVM is unable to boot up properly when doing a hard reboot with the host.
603100	Autoscale not syncing certificate among the cluster members.
606527	GUI and CLI interface dropdown lists are inconsistent.
634245	Dynamic address objects are not resolved to all addresses using Azure SDN connector.
652416	AWS Fabric connector always uses root VDOM even though it is not a management VDOM.
659333	Slow route change for HA failover in GCP cloud.
663276	After cloning the OCI instance, the OCID does not refresh to the new OCID.
668131	EIP is not updating properly on FG-VM Azure.
670166	FG-VM64-KVM configuration revisions lost after upgrading from 6.2.5.

Web Filter

Bug ID	Description
587018	Add URL flow filter counters to SNMP.
610553	User browser gets URL block page instead of warning page when using HTTPS IP URL.
620803	Group name missing on web filter warning page in proxy-based inspection.
629005	foauthd has signal 11 crashes when FortiGate authenticates a web filter category.
659372	Inconsistent behavior between external list and FortiGuard categories/local override.

WiFi Controller

Bug ID	Description
618456	High cw_acd usage upon polling a large number of wireless clients with REST API.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
633089	FortiOS 6.2.6 is no longer vulnerable to the following CVE Reference: • CVE-2020-15937

Known issues

The following issues have been identified in version 6.2.6. To inquire about a particular bug or 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.

Firewall

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

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	The 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/allow list entry, *Mark as Reject* should be grayed out.
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 shows incorrectly when adding 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.
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.
656429	Intermittent GUI process crash if a managed FortiSwitch returns a reset status.
662640	Some GUI pages (dashboard, topology, policy list, interface list) are slow to load on low-end platforms when there are many concurrent HTTPSD requests.
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.
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.
689605	On some browser versions, the GUI displays a blank dialog when creating custom application or IPS signatures. Affected browsers: Firefox 85.0, Microsoft Edge 88.0, and Chrome 88.0.
691277	When logs are retrieved from FortiAnalyzer, the GUI displays the same traffic logs for primary and secondary HA devices.
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.

HA

Bug ID	Description
616345	Secondary device failed to sync with primary device when FGSP is peer configured, but hasync fails to bind socket.
678309	Cluster is out of sync because of `config vpn certificate ca` after upgrade.
703047	`hbdev` goes up and down quickly, then the cluster keeps changing rapidly. `hasync` objects might access invalid cluster information that causes it to crash.

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.
657541	On FG-80D, the IPS engine daemon count drops to 0 when the CPU number is 4.

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.
	Workaround: disable CP or disable the extended database.
	`config ips global`
	`set database regular`
	`set cp-accel-mode none`
	`end`

689590	IP quarantine is not working on FG-80D.

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.

Bug ID	Description
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).
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.

Log & Report

Bug ID	Description
606533	User observes `FGT internal error` while trying to log in or activate FortiGate Cloud from the web UI.
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.

REST API

Bug ID	Description
584631	REST API administrator 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.
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.
669380	Router daemons get stuck after rebooting when executing `get router info routing-table all`.

Bug ID	Description
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
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
649556	FortiNAC requests to FortiGate can timeout on low-end models when there are many concurrent requests.
669436	Filter lookup for Azure connector in *Subnet* and *Virtual Network* sections only shows results for VMSS instance.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.
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
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.
671135	flcfg crashes while configuring FortiSwitches through FortiLink.

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 on contract.
600032	SNMP does not provide routing table for non-management VDOM.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
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.
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.
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.
694202	`stpforward` does not work with LAG interfaces on a transparent VDOM.
695803	Unable to reorder firewall DoS policy in GUI or CLI.
715647	In VWP with `set wildcard-vlan enable`, for some special cases the SKB `headlen` is not long enough for handling. It may cause a protective crash when doing `skb_pull`.

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
595583	Device identification via LLDP on an aggregate interface does not work.
667689	Cannot select remote certificate imported from CLI for SAML IdP.
682711	TACACS users cannot log in via the console.

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.
620654	Spoke dialup IPsec VPN does not initiate connection to hub after FG-VM HA failover in Azure.
640436	FortiGate AWS bootstrapped from configuration does not read SAML settings.
682420	Dialup IPsec tunnel from Azure may not be re-established after HA failover.
685782	HTTPS administrative interface responds over heartbeat port on Azure FortiGate despite `allowaccess` settings.
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.

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.

Built-in AV engine

Resolved engine issues

Bug ID	Description
632769	Fixed UTF-8 characters not displaying properly after archive extraction.
637845	Fixed AV engine inability to properly scan files containing gfxdata payloads.
648561	Fixed AV engine PDF parser crash.
652492	Fixed AV engine crashing when large files are scanned.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
539833	Fix invalid memory access crashes in HTTP fake body.
564595	Application firewall not blocking BitTorrent P2P traffic.
595659	Fix session double release issues in session iterations.
624928	Fix a crash in packet cache caused by sending invalid data buffers.
625371	Fix crash on derived packet processing.
637084	Use existing private keys in FortiGate for certificate resigning.
637553	Web filtering produces rating error logs, despite that FortiGuard connectivity appears to be working.
654363	Security policy action is `deny` in some traffic logs.
654687	`ipsengine` segfault in NGFW policy mode.
656300, 662785	Clean up the rule reference interface.
658482	Fix double initialization in content decoders.
660489	Web filter URL filter check is skipped in flow mode certificate inspection if SNI is not present in TLS client hello.
662573	Fix NULL pointer dereference crash.
662964	PCAP from IPS not dumped as configured in `packet-log-history` and `packet-log-post-attack` settings.
664728	Traffic failing in NGFW policy-based mode when TCP source port range includes a zero value.
668379	DLP triggered by HTTP traffic when only FTP protocol is enabled.
668486	After clearing the server cache, get `Connection reset by peer` message when visiting a URL in a FortiGuard category set to override.
668891	NGFW policy mode allows all services when ICMP is selected in the security policy.
669138	Fix two SSL crashes.
671873	Fix crash in .ZIP file handling.

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.