FortiOS - Release Notes

Version 6.2.5

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

November 2, 2021
FortiOS 6.2.5 Release Notes
01-625-641037-20211102

TABLE OF CONTENTS

Change Log **6**
Introduction and supported models **8**
Supported models 8
Special branch supported models 8
Special notices **10**
New Fortinet cloud services 10
FortiGuard Security Rating Service 10
Using FortiManager as a FortiGuard server 11
FortiGate hardware limitation 11
CAPWAP traffic offloading 12
FortiClient (Mac OS X) SSL VPN requirements 12
Use of dedicated management interfaces (mgmt1 and mgmt2) 12
NP4lite platforms 12
Tags option removed from GUI 12
L2TP over IPsec on certain mobile devices 12
PCI passthrough ports 13
Proxy web filter with SSL inspection may fail for websites that allow TLS versions below 1.3 after upgrading to FortiOS 6.2.5 13
New features or enhancements **14**
Changes in default behavior **15**
Changes in CLI defaults **16**
Upgrade Information **17**
FortiClient Endpoint Telemetry license 17
Fortinet Security Fabric upgrade 17
Minimum version of TLS services automatically changed 18
Downgrading to previous firmware versions 19
Amazon AWS enhanced networking compatibility issue 19
FortiLink access-profile setting 19
FortiGate VM with V-license 20
FortiGate VM firmware 20
Firmware image checksums 21
FortiGuard update-server-location setting 21
FortiView widgets 21
Product integration and support **22**
Language support 24
SSL VPN support 24
SSL VPN standalone client 24
SSL VPN web mode 25
SSL VPN host compatibility list 25
Resolved issues **27**
Anti Spam 27

Anti Virus 27
Application Control 27
Data Leak Prevention 27
Endpoint Control 28
Explicit Proxy 28
Firewall 28
FortiView 28
GUI 29
HA 30
Intrusion Prevention 30
IPsec VPN 30
Log & Report 31
Proxy 31
Routing 32
Security Fabric 32
SSL VPN 32
System 34
Upgrade 35
User & Device 36
VM 36
VoIP 37
Web Filter 37
WiFi Controller 37
Common Vulnerabilities and Exposures 37
Known issues 38
Anti Virus 38
Data Leak Prevention 38
DNS Filter 38
Endpoint Control 38
Explicit Proxy 39
Firewall 39
FortiView 40
GUI 40
HA 41
Intrusion Prevention 42
IPsec VPN 42
Log & Report 43
Proxy 43
REST API 43
Routing 44
Security Fabric 44
SSL VPN 44
Switch Controller 45
System 45

Upgrade 47
User & Device 48
VM 48
Web Filter 49
WiFi Controller 49
Limitations **50**
Citrix XenServer limitations 50
Open source XenServer limitations 50

Change Log

Date	Change Description
2020-08-20	Initial release.
2020-08-24	Removed 640320 from *New features or enhancements*. Updated *Resolved issues* and *Known issues*.
2020-08-26	Added 630070 and 645848 to *Known issues*.
2020-09-10	Added FGR-60F to *Special branch supported models*.
2020-09-17	Updated *Resolved issues* and *Known issues*. Added 617934 to *Special notices*.
2020-09-23	Updated *Resolved issues* and *Known issues*.
2020-10-06	Updated *Resolved issues* and *Known issues*.
2020-10-14	Added FG-80F, FG-80F-BP, and FG-81F to *Special branch supported models*.
2020-10-22	Added FG-1800F, FG-1801F, FG-4200F, and FG-4201F to *Special branch supported models*.
2020-10-27	Added FG-400E-BP to *Special branch supported models*.
2020-10-30	Added FGR-60F-3G4G to *Special branch supported models*.
2020-11-09	Updated *Resolved issues* and *Known issues*.
2020-11-13	Removed 568905 from *Resolved issues*. Added 668625 to *Known issues*.
2020-12-23	Added FG-2600F and FG-2601F to *Special branch supported models*.
2020-12-30	Added FG-80D to *Supported models*.
2021-02-12	Updated *Resolved issues* and *Known issues*.
2021-02-24	Updated *Known issues*.
2021-05-03	Updated *Known issues*. Removed *Built-in IPS engine*.
2021-05-18	Updated *Known issues*.
2021-05-31	Updated *Known issues*.
2021-07-12	Updated *Known issues*.
2021-07-26	Updated *Known issues*.
2021-08-09	Updated *Known issues*.
2021-10-07	Updated *Known issues*.
2021-10-19	Updated *Known issues*.

Date	Change Description
2021-11-02	Updated *Changes in default behavior*.

Introduction and supported models

This guide provides release information for FortiOS 6.2.5 build 1142.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.5 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-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-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 6.2.5. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1142.

FG-80F	is released on build 6801.
FG-80F-BP	is released on build 6801.
FG-81F	is released on build 6801.

FG-400E-BP	is released on build 5848.
FG-1800F	is released on build 5878.
FG-1801F	is released on build 5878.
FG-2600F	is released on build 5884.
FG-2601F	is released on build 5884.
FG-4200F	is released on build 5878.
FG-4201F	is released on build 5878.
FGR-60F	is released on build 5761.
FGR-60F-3G4G	is released on build 5883.

Special notices

- New Fortinet cloud services
- FortiGuard Security Rating Service
- Using FortiManager as a FortiGuard server on page 11
- FortiGate hardware limitation
- CAPWAP traffic offloading
- FortiClient (Mac OS X) SSL VPN requirements
- Use of dedicated management interfaces (mgmt1 and mgmt2)
- NP4lite platforms
- Tags option removed from GUI
- L2TP over IPsec on certain mobile devices on page 12
- PCI passthrough ports on page 13
- Proxy web filter with SSL inspection may fail for websites that allow TLS versions below 1.3 after upgrading to FortiOS 6.2.5 on page 13

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.

Proxy web filter with SSL inspection may fail for websites that allow TLS versions below 1.3 after upgrading to FortiOS 6.2.5

Bug ID	Description
617934	If web filtering is enabled using a proxy-based firewall policy with SSL inspection also enabled, then connections to servers that still support less secure TLS versions may fail. Browser errors seen: Chrome: *ERR_CONNECTION_CLOSED* Firefox: *PR_END_OF_FILE_ERROR* **Workaround**: toggle affected firewall policies to flow-based inspection.

New features or enhancements

Bug ID	Description
480717	Add `config system dedicated-mgmt` to all FortiGate models with mgmt, mgmt1, and mgmt2 ports.
641990	Make the `diagnose wad session list` command available to models without WAN optimization support.

Changes in default behavior

Bug ID	Description

630433	Local category and remote category override can now be controlled at the profile level.
	In proxy mode, `webfilter profile`, `ssl-exempt`, and `proxy-address` have similar behavior in handling local and remote categories. For example, in local category:
	• In 6.0.x, 6.2.x, 6.4.0, and 6.4.1, once a host is configured in the local rating as category 140, it will be always rated as 140 at the global or VDOM level. There is no profile-level option to control it.
	• In 6.4.2, the host will be rated as the configured local rating only when that category is explicitly configured in a web filter profile. This override can be applied to `webfilter profile`, `ssl-exempt`, and `proxy-address`.
	The following is an example configuration for a web filter profile:
	`config webfilter profile`
	`  edit webf-use-local-rating`
	`    config ftgd-wf`
	`      config filters`
	`        edit 1`
	`          **set category 140**`
	`          set action monitor`
	`        next`
	`      end`
	`    end`
	`  next`
	`end`
	The rating in `webfilter profile`, `ssl-exempt`, and `proxy-address` are independent from each other.
	In the GUI, an *Allow* action of a local/remote category when editing a web filter profile is effectively a shortcut to disable the local/remote category overrides.
	For flow mode, only `webfilter profile` is involved, and it has different behavior as the change is in the IPS engine:
	• In 6.2.5 and 6.4.2, the local/remote rating only takes effect when the category is enabled in `webfilter profile`.
	• In 6.2.1-6.2.4 and 6.4.0-6.4.1, currently the local/remote rating is still at the global or VDOM level. After the next IPS engine public release, the behavior will be changed to be the same as 6.2.5/6.4.2.
	There is no change in `ssl-exempt` for FortiGuard with flow mode and the NGFW URL category.

Changes in CLI defaults

Bug ID	Description

613730	Add `subscription-id` attribute for route table in Azure SDN configuration to allow updating a route table in a different subscription.
	`config system sdn-connector`
	`edit "azsdn"`
	`config route-table`
	`edit "xxxxxxxxx-rtb1"`
	`set subscription-id "xxxxxxxxxxxxxxx" <==added`
	`set resource-group "xxxxxxxxx"`
	`config route`
	`edit "internal-forword"`
	`set next-hop "172.28.5.4"`
	`next`
	`end`
	`next`
	`end`
	`end`

613876	Add `dhcp-ra-giaddr` under `ipsec phase1-interface`.
	`config vpn ipsec phase1-interface`
	`edit "1"`
	`set type dynamic`
	`set peertype any`
	`set net-device disable`
	`set mode-cfg enable`
	`set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1`
	`set dpd on-idle`
	`set assign-ip-from dhcp`
	`set dhcp-ra-giaddr <==added`
	`next`
	`end`

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 6.2.5 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 6.2.5. When the Security Fabric is enabled in FortiOS 6.2.5, all FortiGate devices must be running FortiOS 6.2.5.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.5 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 6.2.5 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 6.2.5 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 6.2.5 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 6.2.5, 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 6.2.5.

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 6.2.5 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 0292 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	• 6.00149
IPS Engine	• 5.00218
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 6.2.5. For inquires about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
497024	Flow mode banned word spam filter log is missing the banned word.

Anti Virus

Bug ID	Description
582368	URL threat detection version shows a large negative number after FortiGate reboots.
615805	Device goes into conserve mode due to large files.

Application Control

Bug ID	Description
630075	After upgrading, FortiGate faced an internet access issue when IPS and AC profiles are enabled and the outgoing interface is an npu_vlink.

Data Leak Prevention

Bug ID	Description
582480	scanunit crashes with signal 11 in dlpscan_mailheader when AV scans files via IMAP.

Endpoint Control

Bug ID	Description
608301	EMS serial number format should be flexible.

Explicit Proxy

Bug ID	Description
591012	WAD crashed at wad_disclaimer_get with signal 11 when disclaimer is enabled in proxy policy and the browser is Chrome.
610298	Compare and sync the VSD change in V5.6 to WAD VS.
650540	FortiGate sends traffic to an incorrect port using a wrong source NAT IP address.

Firewall

Bug ID	Description
596633	In NGFW mode, IPS engine drops RPC data channel when IPS profile is applied to a security policy.
603263	Increase the maximum limit for the optional parameters in SCTP INIT packet. After the fix, the maximum limit is 10 instead of 4 parameters.
606962	Timeout value is not reflected correctly to a new session when changing timeout value for `system session-ttl` on FortiGate-HV.
610557	FortiGate VIP object offers weak elliptic curves since VS implementation in WAD for FortiOS 6.0 and above.
615073	FTP session helper does not work when there is reflected (auxiliary) session.
622045	Traffic not matched by security policy when using service groups in NGFW policy mode.

FortiView

Bug ID	Description
573138	When the data source is FortiGate Cloud, there is no paging to load sessions; only entries 1-499 are rendered.

GUI

Bug ID	Description
401862	*Monitor* page display incorrect virtual server entries for IPv6, VIP46, and VIP64; right-clicking gives an error.
493819	Reorder function on *Authentication Rules* page does not work.
513694	User cannot log in to GUI when password change is required and has pre-login or post-login banner enabled or FIPS mode.
564849	HA warning message remains after primary device takes back control.
594534	GUI shows *Invalid LDAP server* error while LDAP query successfully finished.
594702	When sorting the interface list by the *Name* column, the ports are not always in the correct order (port10 appears before port2).
601568	Interface status is not displayed on faceplate when viewing from the *System* > *HA* page.
604682	GUI takes two minutes to load *VPN* > *IPsec Tunnels* for 1483 tunnels.
605496	Configured overlapped subnet on GUI still shows error message after enabling subnet overlap.
614056	Disabling the *Idle Logout* toggle on the *SSL-VPN Settings* page does not change the idle timeout setting, so the change does not persist after clicking *Apply*.
615267	In Firefox, SAML SSO admin cannot create additional SSO admins or normal admins via the GUI.
616878	DHCP relay IP address not showing on *Network* > *Interfaces* page for VLAN interface.
620854	GUI should not add speed to virtual switch member port (FG-101F).
623109	IPS *Filter Details* column is empty when *All* is used.
624551	On POE devices, several sections of the GUI take over 15 seconds to fully load.
628373	Software switch members and their VLANs are not visible in the GUI interfaces list.
633937	GUI is not displaying DHCP configuration if the interface name includes the \ character.
638277	Firewall address group object (including interface subnet) is invisible in *Accessible Networks*.
639756	*Monitor* > *SD-WAN Monitor* keeps loading after disabling VPN member.
642402	LCP-1250RJ3SR-K transceiver shows a warning in the GUI even though it is certified.
644999	Fortinet-sold active direct attached cable (SP-CABLE-ADASFP+) is showing as not certified by Fortinet.
646327	Web filter profile dialog cannot load URL filter table if there are a lot of URL filters.
650800	Unable to delete multiple phase 2 selectors at the same time from the VPN IPsec tunnels dialog.
654339	GUI search does not work in the interface list if DHCP client and range columns are present.

HA

Bug ID	Description
621583	HA cannot display status in GUI when heartbeat cables reconnect.
623642	It takes up to 10 seconds to get NPU VDOM link up when rebooting primary unit.
627610	When HA primary device is down, a time synchronization with NTP servers will be disabled after failback.
631342	FG-100D HA A-P mode not syncing.
637843	HA secondary device is reporting multiple events (DDNS update failed).
638287	`private-data-encryption` causes cluster to be periodically out of sync due to customer certificates.
645293	`traceroute` not working in asymmetric FGSP environment.
656099	mgmt interfaces are excluded for heartbeat interfaces (even if `dedicate-mgmt` is not enabled).

Intrusion Prevention

Bug ID	Description
587363	IPS engine and IPS helper crash with signal 6 (aborted).
595062	SSL offloading randomly does not work when UTM (AV/IPS) is enabled on firewall policy.
631381	RDP NLA authentication blocked by FortiGate when enabling IPS profile in the security group (central NAT).

IPsec VPN

Bug ID	Description
584982	The customer is unable to log in to VPN with RADIUS intermittently.
606129	`iked` crash when proposal is AES-GCM.
607134	Upon reboot, failover or re-negotiation occurs with an active FEC enabled and tunnel traffic can no longer pass.
610390	IKEv2 EAP certificate authentication failings after upgrading from to 6.2.1 to 6.2.3.
610558	ADVPN cannot establish after primary ISP has recovered from failure and traffic between spokes is dropped.

Bug ID	Description
631968	IKE daemon signal 6 crash when `phase1 add-gw-route` is enabled.
634883	IKE crashes at `ike_hasync__xauth`.
635325	Static route for site-to site VPN remains active even when the tunnel is down.

Log & Report

Bug ID	Description
605405	IPS logs are recorded twice with TCP offloading on virtual server.
608565	FortiGate sends incorrect long session logs to FortiGate Cloud.
612779	Reliable syslogd session goes into bad state due to traffic shaper.
616835	Logs from HA secondary unit cannot be uploaded to FortiCloud.
628358	Logs are not generated in GUI and CLI after checking the file system (after power cable disconnected).
635013	FortiOS gives wrong time stamp when querying FortiGate Cloud log view.
643840	`vwlservice` should log the SD-WAN rule and not an internet service; impacts FortiAnalyzer SD-WAN monitor widgets and reports.

Proxy

Bug ID	Description
586909	When CIFS profile is loaded, using MacOS to access Windows Share causes WAD to crash.
612333	In FortiGate with squid configuration (proxy chain), get *ERR_SSL_PROTOCOL_ERROR* when using Google Chrome with certificate/deep inspection.
615791	Abbreviated handshake randomly receives fatal illegal_parameter against zendesk.com services/sites.
617099	WAD crashes every few minutes.
623108	FTP-TP reaches high memory usage and triggers conserve mode.
631723	AV in proxy inspection mode blocks Cisco Webex traffic.
632085	When CIFS profile is loaded, using MacOS (Mojave 10.14) to access Windows 2016 SMB Share causes WAD to crash.
637389	The WAD process is crashing multiple times.
640427	Web proxy WAD crash under WAN Opt auto-active mode.

Routing

Bug ID	Description
602679	Prevent BGP daemon crashing when peer breaks TCP connection.
602826	BGP route is not added into kernel during ADVPN test.
608106	BGP daemon crashes when TCP connection is broken by peer.
611539	Editing/adding any address object that is referenced in policy is generating false positive SD-WAN alert messages.
613716	Local-out TCP traffic changes output interface when irrelevant interface is flapping that causes disconnections.
619343	Cannot ping old VRIPs when adding new VRIPs.
625345	The single BGP update message contains the same prefix in withdrawn routes and NLRI (advertised route).
627951	NTP and FSSO not following SD-WAN rules
628896	DHCP relay does not match the SD-WAN policy route.
629521	SD-WAN IPv6 default route cannot be redistributed into BGP using `set default-originateroutemap6`.
635716	FortiGuard web filter traffic also needs to follow SD-WAN service.

Security Fabric

Bug ID	Description
597139	Crash happens due to segfault in CSF.
609182	*Security Fabric Settings* page sometimes cannot load FortiSandbox URL threat detection version despite FortiSandbox being connected.

SSL VPN

Bug ID	Description
595505	FortiGate does not send client IP address as a framed IP address to RADIUS server in RADIUS accounting request message.
600029	Sending RADIUS accounting interim update messages with SSL VPN client framed IP are delayed.

Bug ID	Description
604772	SSL VPN tunnel is unexpectedly down sometimes when certificate bundle is updated.
606271	Double redirection through SSL web mode not working.
607687	RDP connection via SSL VPN web portal does not work with UserPrincipalName (UPN) and NLA security.
608464	Get 305 error when browsing website through SSL VPN web mode bookmark and sslvpnd crashes.
610579	Videos from live cameras via SSL VPN web mode not working.
617170	https://outlook.office365.com cannot be accessed in SSL VPN web portal.
620508	CLI command `get vpn ssl monitor` displays users from other VDOM.
622068	Adding FQDN routing address in split tunnel configuration injects single route in client for multiple A records.
622110	SSL VPN disconnected when importing or renaming CA certificates.
622871	SSL VPN web mode not displaying full customer webpage after logging in.
623076	Add memory protection for web mode SSL VPN child process (guacd).
623231	Pages could not be shown after logging in to back-end application server.
623379	Memory corrupt in some DNS callback cases causes SSL VPN crash.
624145	An internal website via SSL VPN web portal failed to load an external resource.
624899	Log entry for tunnel stats shows wrong tunnel ID when using RDP bookmark.
624904	The company website is not shown properly in SSL VPN web mode.
625301	Riverbed SteelCentral AppResponse login form is not displaying in SSL VPN web mode.
628821	Internal aixws7test2 portal is not loading in SSL VPN web mode.
629190	After SSL VPN proxy, some JS files of hapi website could not work.
629373	SAML login button is lost on SSL VPN portal.
631130	Internal site http://va***.com not completely loading through SSL VPN web mode bookmark.
633812	For guacd daemon generated for RDP session, it would sometimes be in an unknown state with 100% CPU and could not be released.
634991	Internal server error 500 while accessing contolavdip portal in SSL VPN web mode.
635307	Map could not be displayed correctly in SSL VPN web mode.
636984	Website (pr***.com) not loading properly in SSL VPN web mode.
637018	After the upgrade to 6.0.10/6.2.4/6.4.0, SSL VPN portal mapping/remote authentication is matching user into the incorrect group.
638733	Internal website hosted in bookmark https://in***.cat is not loading completely in SSL VPN web mode.

Bug ID	Description
648369	Some JS files of jira.***.vwg could not run in SSL VPN web mode.
649130	SSL VPN log entries display users from other VDOMs.
654534	SAML authentications occurring through SSL VPN web mode are not completing.

System

Bug ID	Description
503125	FG-100D traffic traversing port1-port16 only saturates CPU0.
567019	CP9 VPN queue tasklet unable to handle kernel NULL pointer dereference at 0000000000000120 and device reboots.
576323	SFP+ 1G speed should be supported on FG-1100E, FG-1800F, FG-2200E, and FG-3300E series.
581496	FG-201E stops sending out packets and NP6lite is stuck.
594871	Potential memory leak triggered by FTP command in WAD.
604613	`sentbyte` of NTP on local traffic log shows as `0` bytes, even though NTP client receives the packet.
607357	High CPU usage issue caused by high depth expectation sessions in the same hash table slot.
607836	Failed to set `ping-option` source to `Auto`.
608442	After a reboot of the PPPoE server, the FortiGate (PPPoE clients, 35 clients) keeps flapping (connection down and up) for a long time before connecting successfully.
609660	NPU offloading enabled dropping traffic from IPsec VPN tunnel remote gateway.
611512	When a LAG is created between 10 GE SFP+ slots and 25 GE SFP28/10 GE SFP+ slots, only about 50% of the sessions can be created. Affected models: FG-110xE, FG-220xE, and FG-330xE.
612302	FortiOS is not sending out IPv6 router advertisements from the link-local addresses added on the fly.
612351	Many `no session matched` logs while managing FortiGate.
613017	`ip6-extra-addr` does not perform router advertisement after reboot in HA.
613136	Uninitialized variable that may potentially cause httpsd signal 6 and 11 crash issue.
615435	Crashes might happen due to CMDB query allocation fail that causes a segfault.
616022	Long delay and cmdbsvr at 100% CPU consumption when modifying address objects and address groups via GUI or REST API.
617134	Traffic not showing statistics for VLAN interfaces base on hardware switch.
617154	Fortinet_CA is missing in FG-3400E.
617409	The FG-800D HA LED is off when HA status is normal.

Bug ID	Description
618762	Fail to detect transceiver on all SFP28/QSFP ports. Affected platforms: FG-3300E and FG-3301E.
620827	Over a period of time, FG-60E goes into memory conserve mode caused by resource leak of sepmd daemon.
623501	FG-80D may fail to boot due to a limitation in the size of the bootloader and kernel.
626371	Request to blocked signature with SSL mirrored traffic capture causes FG-500E to reboot.
632353	Virtual WAN link stops responding after 45 members.
632635	Frame size option in sniffer does not work.
632788	DSL module of FortiWiFi 60E-DSL shows as `not ready` after upgrade.
633102	DHCPv6 client's DUID generated on two different FortiGates match.
634600	FWF-60E-DSL ADSL2+ connection provided by BT in the UK does not work after upgrading from 6.0.9 to 6.2.4.
636069	Unable to handle kernel NULL pointer dereference at 000000000000008f.
637420	`execute shutdown` reboots instead of shutting down on SoC4 platforms.
638041	SFP28 port group (ha1, ha2, port1 and port2) missing `1000full` speed option. Affected platforms: FG-220xE, FG-330xE, FG-340xE, and FG-360xE.
641419	FG-40F LAN interfaces are down after upgrading to 6.2.4 (build 5632).
643188	Interface `forward-error-correction` setting not honored after reboot.
647593	After reboot, `forward-error-correction` value is not maintained as it should be.
647718	VDOM with long name cannot be deleted.
648977	Sometimes when updating the FortiGate license, there is a certificate verification failure.

Upgrade

Bug ID	Description
615972	After upgrading from 6.2.2 to 6.2.3, the description field in the table has disappeared under DHCP reservation.
635589	Upon upgrading to FortiOS 6.2.4, DoS policies configured on interfaces may drop traffic that is passing through the DoS policy configuration. Note that this can occur if the DoS policy is configured in drop or monitor mode. **Workaround:** disable the DoS policy.
649948	Upon upgrading to an affected 6.2 or 6.4 firmware, IKE/IPsec SAs are not synced to the primary when HA `uninterruptible-upgrade` is enabled. As a result, IPsec traffic from a client may be detected as having an invalid SPI until the client starts a new negotiation.

User & Device

Bug ID	Description
591170	Sessions are removed from the session table when FSSO group order is changed.
604844	`auth-concurrent` setting in user group is not working as expected.
605838	Device identification scanner crashes on receipt of SSDP search.
620941	Two-factor authentication using FortiClient SSL VPN and FortiToken Cloud is not working due to push notification delay.
621161	`src-vis` crashes on receipt of certain ONVIF packets.
626532	fnbamd is not sending `Calling-Station-Id` in `Access-Request` for L2TP/IPsec since 5.4.0.
627144	Remote admin LDAP user login has authentication failure when the same LDAP user has local two-factor authentication.
629487	Older FortiGate models do not have CA2 and will cause EMS server authentication to fail.
637577	Inconsistent fnbamd LDAP group match result.
638593	Certificate verification fails if any CA in a peer-provided certificate chain expires, but its cross-signed certificate is still valid in the system trust store.

VM

Bug ID	Description
613730	Unable to update routing table for a resource group in a different subscription with FortiGate Azure SDN.
614038	vMotion causing sessions to be disconnected as it consider sessions stateless.
623376	Cross-zone HA breaks after upgrading to 6.4.0 because upgrade process does not add relevant items under `vdom-exception`.
624657	Azure changes FPGA for Accelerated Networking live and VM loses SR-IOV interfaces.
626705	By assigning port1 as the HA management port, the HA secondary unit node is now able to send system information to the Azure portal through waagent so that up-to-date information is displayed on the Azure dashboard. If port1 is not used as the HA management port, the Azure display and Azure Security Center alerts will not reflect the correct state of the node, which may result in unnecessary alarms.
634499	AWS FortiGate NIC gets swapped between port2 and port3 after FortiGate reboots.
641038	SSL VPN performance problem on OCI due to driver.

VoIP

Bug ID	Description
620742	RAS helper does not NAT the port 1720 in the `callSignalAddress` field of the `RegistrationRequest` packet sent from the endpoint.
630024	voipd crashes repeatedly.

Web Filter

Bug ID	Description
618153	FSSO users cannot proceed on web filter warning page in flow-based inspection.
636754	If the last line in a threat feed does not end with "\n", it is not parsed and is not displayed in the GUI.
657466	`local urlfilter` configuration in a flow mode web filter does not work when the matched FortiGuard category is also enabled in the web filter profile.

WiFi Controller

Bug ID	Description
625326	FortiAP not coming online on FG-PPPoE interface.
641811	In FG-100F/101F with PPPoE interface, the FortiGate could not manage FortiAP.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
606237	FortiOS 6.2.5 is no longer vulnerable to the following CVE Reference: • CVE-2020-6648
618238	FortiOS 6.2 running AV engine version 6.00145 or later is no longer vulnerable to the following CVE Reference: • CVE-2020-9295
634975	FortiOS 6.2.5 is no longer vulnerable to the following CVE Reference: • CVE-2020-12819

Known issues

The following issues have been identified in version 6.2.5. For inquires about a particular bug or to report a 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
582374	License shows expiry date of `0000-00-00`.
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
540091	Cannot access explicit FTP proxy via VIP.
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.
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.
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
635309	When FortiAnalyzer logging is configured using an FQDN domain, the GUI displays a 500 error message on the FortiView *Compromised Hosts* page.
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.
673225	FortiView *Top Traffic Shaping* widget does not show data for outbound traffic if the source interface's role is WAN. The 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 are incorrectly filtered when there are two *Action* filters and one of them contains "-".
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.
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.
612236	RADIUS test fails from the GUI as it does not use the configured *Authentication method*, and authentication fails; test passes on the CLI.
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.
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.

Bug ID	Description
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.
656429	Intermittent GUI process crash if a managed FortiSwitch returns a reset status.
660165	When creating SD-WAN rules in the GUI, the destination interface preference is not saved when the strategy is manual.
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.
663351	Connectivity test for RADIUS server using CHAP authentication always returns failure.
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.
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.
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.
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.
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
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.
634604	SCTP sessions are not fully synchronized between primary and secondary devices in version 5.6.11 on FG-3240C.
639307	Both primary and secondary consoles keep printing `get_ha_sync_obj_sig_4dir: stat /etc/cert/ca/5c44d531.0 error 2`.

Bug ID	Description
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.
678309	Cluster is out of sync because of `config vpn certificate ca` after upgrade.

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.
655371	Logging is intermittent for FortiGate IDS passive in one-armed sniffer mode.
657541	On FG-80D, the IPS engine daemon count drops to 0 when the CPU number is 4.
689590	IP quarantine is not working on FG-80D.

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.
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).
659535	Setting same `phase1-interface` in SD-WAN member and SD-WAN zone causes iked watchdog timeout.

Log & Report

Bug ID	Description
606533	User observes `FGT internal error` while trying to log in or activate FortiGate Cloud from the web UI.
634947	rlogd signal 11 crashes.
641450	The miglogd processes is bound to busy CPUs, even though there are other completely idle CPUs available.
650325	The miglogd process crashes with signal 11.

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.
617322	DLP FTP proxy with splice option sends delete command to server before data transfer completes.
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.
648831	WAD memory leak caused by Kerberos proxy authentication.
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.

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.
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.
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 crashes.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
629723	SDN dynamic address import is too slow, and HA sync may miss endpoints in high scale and stress conditions.
649556	FortiNAC requests to FortiGate can timeout on low-end models when there are many concurrent requests.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.
548599	SSL VPN crashes on parsing some special URLs.
620793	A page inside a bookmark not opening in SSL VPN web mode.
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.

Bug ID	Description
631082	FortiManager tabs/page do not load when accessed via SSL VPN web mode.
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.
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.
648433	Internal website loading issue in SSL VPN web portal for ca***.fr.
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.
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
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.
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
464340	EHP drops for units with no NP service module.
574716	The ospfNbrState OID takes too long to update.

Bug ID	Description
578031	FortiManager Cloud cannot be removed once the FortiGate has trouble on contract.
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.
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.
600032	SNMP does not provide routing table for non-management VDOM.
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.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
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.
628642	Issue when packets from same session are forwarded to each LACP member when NPx offload is enabled.
630861	Support FortiManager when `private-data-encryption` is enabled in FortiOS.
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.
642327	FortiGate unable to boot with kernel panic by cmdbsvr when VLAN is configured on redundant interface with non-NPU port.
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. **Workaround**: back up the 6.4.0 configuration, perform a clean installation via TFTP of FortiOS 6.4.2, and restore the 6.4.0 configuration.
645363	SNMP monitoring does not provide the SD-WAN member interface name.

Bug ID	Description
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.
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.
657629	ARM-based platforms do not have sensor readings included in SNMP MIBs.
658933	Under some circumstances, it was possible for Update D to create zombie processes.
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.
663603	The maximum number of IPS supported by each NTurbo load balancer should be 7 instead of 8 on FG-3300E and FG-3301E.
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.
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.
692943	If an updated FFDB package is found, crash may happen at `init_ffdb_map` if it is called when `ffdb_map` or `ffdb_app` is already in the process of being parsed, especially in HA.
694202	`stpforward` does not work with LAG interfaces on a transparent VDOM.

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`

Bug ID	Description
	edit <id> set admin enable next end

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.
595583	Device identification via LLDP on an aggregate interface does not work.
658982	ADVPN IKEv2 certificate authentication does not work with OCSP check when certificates do not contain OCSP path.
659456	REST API authentication fails for API user with PKI group enabled due to fnbamd crash.

VM

Bug ID	Description
587180	FG-VM64-KVM is unable to boot up properly when doing a hard reboot with the host.
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.
603100	Autoscale not syncing certificate among the cluster members.
605511	FG-VM-GCP reboots a couple of times due to kernel panic.
606527	GUI and CLI interface dropdown lists are inconsistent.
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.
634245	Dynamic address objects are not resolved to all addresses using Azure SDN connector.
640436	FortiGate AWS bootstrapped from configuration does not read SAML settings.
652416	AWS Fabric connector always uses root VDOM even though it is not a management VDOM.

Bug ID	Description
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.
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
670166	FG-VM64-KVM configuration revisions lost after upgrading from 6.2.5.
685782	HTTPS administrative interface responds over heartbeat port on Azure FortiGate despite `allowaccess` settings.

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.

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.