FortiOS - Release Notes

Version 6.2.4

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

May 13, 2020
FortiOS 6.2.4 Release Notes
01-624-603558-20200513

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-05-12	Initial release.
2020-05-13	Updated *Known issues* and *Resolved issues*. Removed *Downgrading from 6.4.0 to 6.2.4* from *Upgrade Information*.

Introduction and supported models

This guide provides release information for FortiOS 6.2.4 build 1112.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.4 supports the following models.

FortiGate	FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30E-MG, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-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-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

FG-80D will be released at a future date. Please see bug 623501 in the *Known issues* section.

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.

Application group improvements

Bug ID	Description
565309	*Application Group* improvements.

NGFW mode

Bug ID	Description
584314	NGFW mode should have a link to show list of all applications.

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.

New features or enhancements

Bug ID	Description
578099	FortiAP profile support for FortiAP-231E NPI model. CLI changes: • Added `wtp-profile` support for FAP-231E NPI platform. • Multimode: single 5G and dual 5G same as U43xF with minor differences: • Single 5G • Radio 1 operates at 2.4 GHz • Radio 2 operates at 5 GHz • Radio 3 set to monitor mode • Dual 5G • Radio 1 operates at 5 GHz and uses the higher spectrum of channels (>= 64) • Radio 2: operates at 5 GHz and uses the lower spectrum of channels (< 64) • Radio 3: can be set to AP mode • New `wtp-profile` platform property `ddscan`. • FortiGate will configure DFS channels on FAP-231E with region code E, I, V, Y, and D. • Default mode for 3-radio AP models set to single 5G . GUI changes: • Added GUI support for FAP-231E platform: • New GUI option, *Dedicated scan*, which is counterpart of `ddscan` platform property. • When dedicated scan is enabled: • Monitor mode becomes exclusive to radio 3 • No AP mode for radio 3, even in dual 5G • No WIDS profile setting for radio 1 and 2 API changes: • /api/v2/monitor/wifi/ap_platforms • Radio property changed from object to array to accommodate for multimode platforms. First element is single 5G, and second is dual 5G platform radio configuration. For non-multimode platforms, array is of length 1.
599925	Add option to enable/disable DFS zero-wait functionality on FAP-U platforms (the default is `enable`). `config wireless-controller wtp-profile` `edit "FAPU431F-default"` `config platform` `set type U431F` `end` `set handoff-sta-thresh 30` `config radio-1`

Bug ID	Description
	`` set band 802.11ax-5G set zero-wait-dfs disable end config radio-2 set band 802.11ax end config radio-3 set mode monitor end next end ```
600474	Add `local-standalone` that can be enabled on local-bridge mode VAP with external captive portal type. ``` config wireless-controller vap edit "lo-sd-cap" set ssid "local-stand-cap" set security captive-portal set external-web "https://172.18.56.163/portal/index.php" set radius-server "peap" set local-standalone enable set local-bridging enable set portal-type external-auth next end ```
605709	Add new profiles for FAP-431F and FAP-433F NPI platforms. ``` config wireless-controller wtp-profile edit "FAP433F-default" config platform set type 433F set ddscan enable end set handoff-sta-thresh 55 config radio-1 set band 802.11ax,n,g-only end config radio-2 set band 802.11ax-5G end config radio-3 set mode monitor end next edit "FAP431F-default" config platform ```

Bug ID	Description
	set type 431F set ddscan enable end set handoff-sta-thresh 55 config radio-1 set band 802.11ax,n,g-only end config radio-2 set band 802.11ax-5G end config radio-3 set mode monitor end next end
609167	FortiGate will assign a report index for each managed FAP so the FAP can send client, rogue AP, and rogue station information in order. This avoids a burst in CPU usage to deal with report from all FAPs at the same time. This is not a visible functionality. It is a back end optimization feature.
612176	Support setting DiffServ code for SD-WAN health check probe packets. When an SD-WAN health check packet is sent out, the differentiated services code point (DSCP) can be set with a CLI command (`set diffservcode`, range 000000–111111). `config system virtual-wan-link` `config health-check` `edit h1` `...` **`set diffservcode Differentiated services code point (DSCP) in the IP header of the probe packet.`** `...` `next` `end` `end`

Changes in CLI defaults

Bug ID	Description
599034	Remove `top-summary` from `diagnose system`. `diagnose system ?` `...` **`top-summary Show top aggregated processes information. <==removed`**
600830	Add `probe-timeout` under `virtual-wan-link health-check` and `system link-monitor`. `config system virtual-wan-link` `  config health-check` **`  set probe-timeout 500 <==added`** `  end` `end`
608942	Add `force-inclusion-ssl-di-sigs` under application profile. `config application list` `  edit "app-list-1"` **`  set force-inclusion-ssl-di-sigs disable <==added`** `  next` `end`

Changes in default values

Bug ID	Description
588382	Single 5G mode is the default setting for tri-radio AP models (FAP-U431F/U433F).

Changes in table size

Bug ID	Description
599271	Except for desktop models, all other platforms' table size of VIP real servers are increased as follows: • 1U platforms increased from 8 to 16 • 2U platforms increased from 32 to 64 • High-end platforms increased from 32 to 256
609785	Update number of supported FortiSwitch models per FortiGate platform.

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

- FortiAnalyzer 6.2.3
- FortiClient EMS 6.2.0
- FortiClient 6.2.2
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.9 and later

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

If the Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.4. When the Security Fabric is enabled in FortiOS 6.2.4, all FortiGate devices must be running FortiOS 6.2.4.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.4 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 6.2.4 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 6.2.4 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 6.2.4 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 6.2.4, 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 6.2.4.

To configure `local-access` profile:

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

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

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

FortiGate VM with V-license

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

To enable `split-vdom`:

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

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

FortiView widgets have been rewritten in 6.2.4. FortiView widgets created in previous versions are deleted in the upgrade.

Product integration and support

The following table lists FortiOS 6.2.4 product integration and support information:

Web Browsers	• Microsoft Edge 44 • Mozilla Firefox version 71 • Google Chrome version 78 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 42 • Mozilla Firefox version 71 • Google Chrome version 78 • 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 0291 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	• 6.00144
IPS Engine	• 5.00209
Virtualization Environments	
Citrix	• XenServer version 7.1
Linux KVM	• Ubuntu 18.04.3 LTS • QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21) • libvirtd (libvirt) 4.0.0
Microsoft	• Hyper-V Server 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN standalone client

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

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04 / 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 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
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 6.2.4. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
557998	Quarantined CDR files cannot be downloaded. Encountered 404 error when clicking *Archived File*.
563250	Shared memory does not empty out properly under /tmp.
594696	Sample file eicar.exe cannot pass through SMTPS, POP3S, or IMAPS with deep inspection and flow enabled on IPv6 policy.

Data Leak Prevention

Bug ID	Description
563447	Cannot download DLP archived file from GUI for HTTPS, FTPS, SMTP and SMTPS.
571171	Excessive false positives for credit card DLP profiles.
574722	DLP blocks Gmail with deep inspection.
591178	WAD fails to determine the correct file name when downloading a file from Nextcloud.

Explicit Proxy

Bug ID	Description
589166	EPSV does not work when using an FTP proxy.
594580	FTP traffic over HTTP explicit proxy does not generate traffic logs once receiving error message.
594598	Enabling proxy policies (+400) increases memory by 30% and up to 80% total.
603707	The specified port configurations of `https-incoming-port` for `config web-proxy explicit` disappeared after rebooting.
605209	LDAP ignores `source-ip` with web proxy Kerberos authentication.

Firewall

Bug ID	Description
593103	When a policy denies traffic for a VIP and `send-deny-packet` is enabled, ICMP unreachable message references the mapped address, not the external.
595044	Get new CLI signal 11 crash log when performing `execute internet-service refresh`.
596218	ISDB ID is missing when configuring internet service group objects.
598559	ISDB matches all objects and chooses the best one based on their weight values and the firewall policy.
599253	GUI traffic shaper *Bandwidth Utilization* should use KBps units.
600051	Cannot establish the connection to the real servers using VIP server load-balancing after upgrading to FortiOS 6.2.2.
600644	IPS engine did not resolve nested address groups when parsing the address group table for NGFW security policies.
601331	Virtual load-balance VIP and intermittent HTTP health check failures.
604886	Session stuck in proto_state=61 only when flow-based AV is enabled in the policy.
611840	Firewall policy search with decimal in the name fails in GUI.

FortiView

Bug ID	Description
592309	FortiView physical topology page cannot load; get *Failed to get FortiView data* error message.

GUI

Bug ID	Description
557786	GUI response is very slow when accessing *IPsec Monitor* (api/v2/monitor/vpn/ipsec is taking a long time).
565309	Application groups improvements.
579711	Cannot run *Security Rating* due to disk issue (`diagnose security-rating clean` fails).
584314	NGFW mode should have a link to show all applications in the list.
585055	High CPU utilization by httpsd daemon if there are too many API connections.

Bug ID	Description
585924	Wrong traffic shaper bandwidth unit on 32-bit platform GUI pages.
589709	Status icon in *Tunnel* column on *IPsec Tunnels* page should be removed.
593624	GUI behavior is different with local user using super admin profile and TACACS user using super admin profile.
593899	Upgrading from build 0932 to build 1010 displays *Malware Hash Threat Feed is not found or enabled* error.
598247	One-minute memory; *CPU* and *Sessions* widgets stopped updating after system entered and exited conserve mode.
598725	Login page shows random characters when system language is not English.
599245	Nessus vulnerability scan tool reported more medium level vulnerabilities for 6.2.3 compared with the 6.2.2 result.
599284	`pyfcgid` crashed with `signal 11 (Segmentation fault) received`.
599401	FortiGuard quota category details displays *No matching entries found* for local category.
599612	GUI should allow user to create redundant IPsec tunnel over different interface to the same remote gateway.
601653	When deleting an AV profile in the GUI, there is no confirmation message prompt.
602637	*Block intra-zone traffic* toggle button function is inverted in FortiOS 6.2.3.
602692	*Security Rating* result for SSL VPN certificate fails when using a 384-bit elliptic curve certificate.
603583	Data source is missing in child table entries in a complex type property.
603913	GUI should add interface value check when creating a new zone.
605493	Admin cannot log in to FortiGate GUI.
605677	System goes into conserve mode when editing ISDB entries through GUI.
606074	*Interfaces* is missing in the GUI in sections for *IPv4 Policy* and *SSL-VPN Settings* after upgrading from 6.2.2 to 6.2.3.
606394	DPD setting in GUI cannot be reflected correctly when *Dialup User* and *On Demand* are set by the IPsec wizard.
607296	Firewall address page keeps loading addresses with read-write permission.
607972	FortiGate enters conserve mode when accessing Amazon AWS ISDB object.
609064	*Revoke Token* in GUI reports URL not found on server.
610181	FG-OPC-ONDEMAND (FGVMPG license) shows FortiCare is not supported even though the license was registered in FortiCare.
610573	When saving configuration under global interface, explicit proxy settings are removed.
611436	FortiGate displays a hacked web page after selecting an IPS log.
615085	Slow GUI response with httpsd intermittently consuming high CPU when GUI is accessed.

Bug ID	Description
615462	GUI takes 10-15 seconds to load *Device Inventory*, *IPv4 Policy*, and *Interfaces* pages.
617364	GUI does not list AliCloud SDN address filter.

HA

Bug ID	Description
530215	`application hasync` returns "*** signal 11 (Segmentation fault) received ***".
588908	FG-3400E hasync reports the network is unreachable.
596575	HA active-active master attempts to steer HTTP and SMTP sessions to slave unit over NPU-VLINK interfaces.
596837	Deleting tunnel on master via API call will not delete it from the slave unit.
598937	Local user creation causes HA to be out of sync for several minutes.
601550	Application `hasync` crashes several times.
602266	The configuration of the SD-WAN interface gateway IP should not sync.
602406	In a FortiGate HA cluster, performance SLA (SD-WAN) information does not sync with the slave unit.
613714	HA failover takes over one minute when monitored aggregate interface goes down on master.
621621	Ether-type HA cannot be changed.

Intrusion Prevention

Bug ID	Description
605610	*Security Policy* page is slow to load due to empty security firewall statistic returning from IPS engine.
608501	IPS forwards attacks that are previously identified as dropped.

IPsec VPN

Bug ID	Description
516029	Remove the IPsec global lock.

Bug ID	Description
557812	IPsec does not support the new `interface-subnet` type in its `phase2-interface` and `ipv4-split-include` settings for dialup VPN.
589096	In IPsec after HA failover, performance regression and IKESAs are lost.
590633	Packet loss observed after ADVPN shortcut is created.
594962	IPsec VPN IKEv2 interoperability issue when the FortiGate uses a group as P2 selectors with a non-FortiGate in a remote peer gateway.
595810	Unable to reach network resources via L2TP over IPsec with WAN PPPoE connection.
596429	Traffic unable to pass through for certain phase 2 selectors when there is double SA.
597748	L2TP/IPsec VPN disconnects frequently.
599471	IKEv2 responder can delete static selectors when local narrowing occurs.
602240	IKEv2 EAP-TLS handshake detected retransmit of client, but FortiGate does not retransmit its response.
603090	The OCVPN log file was not closed or properly trimmed due to the incorrect state_refcnt. The OCVPN log file stayed open, grew extremely large, and was never trimmed.
604334	L2TP disconnection when transferring large files.
604923	IKE memory leak when IKEv2 certificate subject alternative name/peer ID matching occurs.
607212	IKEv2 DPD is not triggered if network overlay network ID was mismatched when first configured.
609033	After two HA failovers, one VPN interface member of SD-WAN cannot forward packets.
611148	L2TP/IPsec does not send framed IP address in RADIUS accounting updates.
612319	MTU calculation of shared dynamic phase 1 interface is too low compared to its phase 2 MTU and makes fragmentation high.
615360	OCVPN secondary hub cannot register.
622506	L2TP over IPsec tunnel established, but traffic cannot pass because wrong interface gets in route lookup.

Log & Report

Bug ID	Description
593557	Logs to syslog server configured with FQDN addresses fail when the DNS entry gets updated for the FQDN address.
595151	Log filter for user name in UPN format is not consistent when the log location is set to FortiAnalyzer and local disk.

Bug ID	Description
602459	GUI shows *401 Unauthorized* error when downloading forward traffic logs with the time stamp as the filter criterion.
605174	Incorrect `sentdelta/rcvddelta` in traffic log statistics for RTSP sessions.

Proxy

Bug ID	Description
561552	WAD crashed with signal 6 (MAPI/RPC).
594829	FTP connection is not working with AV profile in proxy inspection mode when FTP user name contains an @.
610466	Multiple WAD crash on FG-500D after upgrading from 6.2.3 (`wad_url_filter_user_cat_load_entry.constprop.7`).

REST API

Bug ID	Description
599516	When managing FortiGate via FortiGate Cloud, sometimes user only gets read-only access.

Routing

Bug ID	Description
580207	Policy route does not apply to local-out traffic.
593951	Improve algorithm to distribute ECMP traffic for source IP-based/destination IP-based.
597733	IPv6 ECMP routes cannot be synchronized correctly to HA slave unit.
598665	BGP route is in routing table but not in FIB (kernel routing table).
599667	OSPF over ADVPN flapping after shortcut tunnel established.
599884	Traffic not following SD-WAN rules when one of the interfaces is VLAN.
600332	SD-WAN GUI page bandwidth shows 0 issues when there is traffic running.
600830	SD-WAN health check reports have packet loss if response time is longer than the check interval.
600995	Policy routes with large address groups containing FQDNs no longer work after upgrading to 6.2.2.

Bug ID	Description
602223	SD-WAN route is not added in routing table when the SD-WAN interface members are IPv4 over IPv6 IPsec.
602679	Prevent BGP daemon crashing when peer breaks TCP connection.
603063	Locally originated traffic on non-default VRF may follow route on VRF 0 when there are routes with the same prefix on both VRFs.
604390	FortiOS 6.2.3 by default drops reply packets received from a different interface (unlike 6.2.2).

Security Fabric

Bug ID	Description
586024	Automation stitch cannot execute shutdown command when FortiGate enters kernel conserve mode.
588262	IP address *Threat Feed* fabric connector not working.
599474	FortiGate SDN connector not seeing all available tag name-value pairs.
604670	Time zone of scheduled automation stitches will always be taken as GMT-08:00 regardless of the system's timezone configuration.

SSL VPN

Bug ID	Description
556657	Internal website not working through SSL VPN web mode.
561585	SSL VPN does not correctly show Windows Admin center application.
563022	SSL VPN LDAP group object matching only matches the first policy; is not consistent with normal firewall policy.
582115	Third-party (Ultimo) web app does not load over SSL VPN web portal.
582265	RDP sessions are terminated (disconnect) unexpectedly.
587300	In web mode, third-party webpage stuck on loading animation; JavaScript error in console.
587732	The SSL VPN web mode SSH widget is not connecting to the SSH server.
588066	SSO for HTTPS fails when using "\" (backslash) with the domain\username format.
588587	Different portals of SIPLAN COMPESA do not show properly in web mode.
593367	SSL VPN bookmark does not load after clicking from the portal.

Bug ID	Description
593621	Website not fully loading through web portal bookmark; loads correctly with iPad user agent.
595627	Cannot access some specific sites through SSL VPN web mode.
596296	SSL VPN fails 90% when connecting with FortiClient.
596352	SAML user name is not correctly recorded in logs when logging in to SSL VPN portal via SSO entry, and history cannot be shown.
596412	Not possible to download PDF file after connecting to portal through SSL VPN bookmark.
596441	FortiOS does not correctly re-write the Exchange OWA logoff URL when accessed via SSL VPN bookmark.
596757	SSL VPN connection stuck at 95% or 98%.
596846	Unable to deauthenticate FSSO user in GUI, but it works in CLI.
597336	Webpage does not load properly through SSL VPN web mode (fails to show CAPTCHA).
597566	Add SSL VPN SSO user logged in from SAML response.
597634	In SSL VPN web mode, internal web services not working and tunnel mode is working fine.
597658	Internal custom web application page running on Apache Tomcat is not displaying in SSL VPN web mode.
598659	SSL VPN daemon crash.
598660	Internal website is not accessible from SSL VPN as the URL is being modified.
599394	SSL VPN web portal bookmarks are not full loading for Vivendi SelfService application.
599658	GUI is not rendered well by SSL VPN portal when using domain and user to log in.
599668	In SSL VPN web mode, page keeps loading after user authenticates into internal application.
599671	In SSL VPN web mode, cannot display complete content on page, and cannot paste or type in the comments section.
599777	Problem with ratm.avanzasa.com portal accessed via SSL VPN web mode.
599960	RADIUS user and local token push cannot log in to SSL VPN portal/tunnel when the password needs to be changed.
600029	Sending RADIUS accounting interim update messages with SSL VPN client framed IP are delayed.
600103	Sslvpnd crashes when trying to query a DNS host name without a period (.).
601084	Site in .NET framework 4.6 or 4.7 not loading in SSL VPN web mode.
601867	SSL VPN web mode cannot open DFS share subdirectories, gives invalid HTTP request message.
602392	Cannot access remote site using SSL VPN web mode after upgrading to FOS 6.2.2.
602645	SSL VPN synology NAS web bookmark log in page does not work after upgrading to 6.2.3.
603518	Internal website not working in SSL VPN web mode; cannot load ESS/MSS page.

Bug ID	Description
603779	Chinese characters are garbled when downloading from SMB/CIFS in SSL VPN web mode.
603817	Internal website is not shown properly in SSL VPN web mode.
603957	SSL VPN LDAP authentication does not work in multiple user group configurations after upgrading the firewall to 6.0.7.
604882	Internal SAP website not working in SSL VPN web mode.
605110	Mobile token is not required when LDAP user and LDAP group are set in SSL VPN policy together.
605699	Internal HRIS website dropdown list box not loading in SSL VPN web mode.
607413	SMB/CIFS bookmark name gets scrambled if it contains special characters like space, backslash, colon, etc.
608453	Internal website is not accessible from SSL VPN due to some Sage X3 JS files with errors.
610564	RDP over web mode SSL VPN to a Windows Server changes the time zone to GMT.
616879	Traffic cannot pass through FortiGate for SSL VPN web mode if the user is a PKI peer.
613641	SSL VPN web mode custom FortiClient download URL with %s causing sslvpnd to crash.
621270	SSL VPN user groups are corrupted in auth list when the user is a member of more than 100 groups.
624197	SSL VPN web mode does not completely load the redirected corporate SSO page when accessing an internal resource.
624904	The Saudi Arabian Airlines website is not shown properly in SSL VPN web mode.
625338	sslvpnd crashing with signal 7 on get_free_idx.
625554	SSL VPN connection was used when the DTLS UDP packet process failed and connection was destroyed.

Switch Controller

Bug ID	Description
517663	On a managed FortiSwitch already running the latest GA image, *Upgrade Available* is shown.
601547	Unable to push user group configuration from FortiGate to FortiSwitch, and `user.group` configuration is deleted.
607707	Unable to push configuration changes from FortiGate to FortiSwitch.
608231	LLDP policy did not download completely to the managed FortiSwitch 108Es.
613323	FortiSwitch trunk configuration sync issue after FortiGate failover.

System

Bug ID	Description
515201	FortiGate cannot display the script name from FortiManager.
527459	SSDN address filter unable to handle space character.
576337	SNMP polling stopped when FortiManager API script executed onto FortiGate.
582498	Traffic can be offloaded to both NTurbo and NP6 when DOS policy is applied on ingress/egress interface in a policy with IPS.
585053	NP6 VLAN LACP-based interface RX/TX counters not increasing.
586990	Customer with FG-50E getting high CPU with 6.2.1.
589079	QSFP interface goes down when the `get system interface transceiver` command is interrupted.
589723	Wrong source IP is bound for `config system fortiguard`.
590021	Enabling `auto-asic-offload` results in keeping `action=deny` in traffic log with an accept entry.
590423	FortiManager needs patch and minor number to update global database when FortiGate firmware upgrade does not trigger an auto-retrieve configuration.
592148	Issue with TCP packets when traversing the virtual wire pair in transparent mode.
592570	VLAN switch does not work on FG-100E.
592827	FortiGate is not sending DHCP request after receiving offer.
593426	Remove DST for Brazil.
594018	Update daemon is locked to one resolved update server.
594577	Out of order packets for an offloaded multicast stream.
594865	`diagnose internet-service match` does not return the IP value of the IP reputation database object.
595338	Unable to execute `ping6` when configuring `execute ping6-options tos`, except for `default`.
595467	Invalid multicast policy created after transparent VDOM restored.
598527	ISDB may cause crashes after downgrading FortiGate firmware.
602523	DDNS `monitor-interface` uses the monitored interface if DDNS services other than FortiGuard DDNS are used.
602548	Some of the clients are not getting their IP through DHCP intermittently.
603194	NP multicast session remains after the kernel session is deleted.
603551	DHCPv6 relay does not work on FG-2200E.

Bug ID	Description
604550	Locally-originated DHCP relay traffic on non-default VRF may follow route on VRF 0.
604699	Header line that is not freed might cause system to enter conserve mode in a transparent mode deployment.
606597	When changing time zone on FG-101E, get *Failed to set SMC timezone* message.
607015	More than usual NTP client traffic caused by frequent DNS lookups and NTP sync for new servers, which happens quite often on some global NTP servers.
607452	Automatically logged out of CLI when trying to configure STP due to /bin/newcli crash.
610900	Low throughput on FG-2201E for traffic with ECN flag enabled.
610903	SMC NTP functions are enabled on some of the models that do not support the feature.
612113	xcvrd attaches shared memory multiple times causing huge memory consumption.
621771	FortiGate cannot be accessed by ping/telnet/ssh/capwap in transparent VDOM.
623113	FortiGate not entering A records in shadow DNS database for cross-subdomain CNAME requests.
626785	FG-101F should support the same WTP size (128) as FG-100F.

Upgrade

Bug ID	Description
618809	Boot up may fail when downgrading from FOS 6.4.0 to 6.2.3.

User & Device

Bug ID	Description
573317	SSO admin with a user name over 35 characters cannot log in after the first login.
592047	GUI RADIUS test fails with `vdom-dns` configuration.
593361	No source IP option available for OCSP certificate checking.
594863	UPN extraction does not work for particular PKI.
596844	Admin GUI login makes the FortiGate unstable when there are lots of devices detected by device identification.
605206	FortiClient server certificate in FSSO CA uses weak public key strength of 1024 bits and certificate expiring in May 2020.

Bug ID	Description
605404	FortiGate does not respond to disclaimer page request when traffic hits a disclaimer-enabled policy with thousands of address objects.
605437	FortiOS does not understand CMPv2 `grantedWithMods` response.
605950	RDP sessions are terminated (disconnect) unexpectedly.
609655	Captive portal exemption after upgrading the device from 6.2.2 to 6.2.3.

VM

Bug ID	Description
575346	`gui-wanopt` cache missing under system settings after upgrading a FortiGate VM with two disks.
594248	Enabling or disabling SR-IOV under vNIC creates duplicate MAC addresses and extra interfaces on the FortiGate.
597003	Unable to bypass self-signed certificates on Chrome in macOS Catalina.
598419	Static routes are not in sync on FortiGate Azure.
599430	FG-VM-AZURE fails to boot up due to `rtnl_lock` deadlock.
600975	Race condition may prevent FG-VM-Azure from booting up because of deadlock when processing NETVSC offering and vPCI offering at the same time.
601357	FortiGate VM Azure in HA has unsuccessful failover.
601528	License validation failure log message missing when using FortiManager to validate a VM.
603365	HA slave member instance shuts down due to RAM difference after stopping/starting the cluster instances.
603599	VIP in autoscale on GCP not syncing to other nodes.
605103	E1000 network adapter will be deleted if there is a VMXNET3 network adapter.
605435	API call to associate elastic IP is triggered only when the unit becomes the master.
606439	License validation failure log message missing when using FortiManager to validate VM.
609283	IP pools are synchronized in FortiGate Azure HA.
612611	Very hard to download image for FG-AWSONDEMAND from FDS.
614544	AWS VM sometimes could not get fdsm image list from FDS.
622031	AZD keeps crashing if Azure VM contains more than 15 tags.

VoIP

Bug ID	Description
599117	`voipd` process crash.
601275	MGCP session helper does not NAT the MGCP body.

Web Filter

Bug ID	Description
551956	Proxy web filtering blocks innocent sites due to `urlsource="FortiSandBox Block"`.
593203	Cannot enter a name for a web rating override and save—error message appears when entering the name.
606965	Unable to whitelist specific YouTube channel when all other YouTube channels or videos are blocked.

WiFi Controller

Bug ID	Description
563630	Kernel panic observed on FWF-60E.
594170	FortiAPs not shown in the GUI.
595653	FortiGate in transparent mode cannot manage FortiAP devices successfully.
599690	Unable to perform COA with device MAC address for 802.1x wireless connection when `use-management-vdom` is enabled.
601012	When upgrading from 5.6.9 to 6.0.8, channels 120, 124, and 128 are no longer there for NZ country code.
608717	Packet loss over CAPWAP tunneled SSID.
615219	FortiGate cannot create WTP entry for FortiAP in transparent mode.

Known issues

The following issues have been identified in version 6.2.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

DNS Filter

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

Explicit Proxy

Bug ID	Description
540091	Cannot access explicit FTP proxy via VIP.

GUI

Bug ID	Description
354464	*AntiVirus* profile in GUI should not override quarantine archive value.
514632	Inconsistent `Refcnt` value in GUI when using ports in HA `session-sync-dev`.
517744	Widget for CPU memory and sessions does not show real time diagram in 12-hours and 24-hours mode.
529094	*Anti-Spam Black White List Entry* in GUI permits action *Mark as Reject* in GUI when it should not.
535099	GUI should add support for new MAC address filter in SSID dialog page.
541042	Log viewer forward traffic cannot support double negate filter (client side issue).
564849	HA warning message, *This FortiGate has taken over for the master*, remains after master takes back control.
584915	*OK* button missing on all pages (policy, interface, system settings) on Android mobile.
584939	VPN event logs shows incorrectly when adding two action filters and if the filter action filter contains "-".

Bug ID	Description
589709	Status icon in *Tunnel* column on *IPsec Tunnels* page should be removed.
601568	Interface status is not displayed on faceplate when viewing from the *System* > *HA* page.
601653	When deleting an AV profile in the GUI, there is no confirmation message prompt.

HA

Bug ID	Description
596551	Syncing problem after restoring one VDOM configuration.

Intrusion Prevention

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

IPsec VPN

Bug ID	Description
592361	Cannot pass traffic over ADVPN if: `tunnel-search` is set to `nexthop`, `net-device disable`, `mode-cfg enable`, and `add-route disable`.

Log & Report

Bug ID	Description
606533	User observes `FGT internal error` while trying to log in from the web UI.
608565	FortiGate sends incorrect long session logs to FortiGate Cloud.

Proxy

Bug ID	Description
575224	WAD high memory usage from worker process causing conserve mode and traffic issues.
582475	WAD is crashing with signal 6 in `wad_fmem_free` when processing SMB2/CIFS.
588661	Customer had issue accessing the HTTPS website after enabling the proxy web filter.

REST API

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

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
602826	BGP route is not added in to kernel during ADVPN test.

Security Fabric

Bug ID	Description
585354	After enabling FortiTelemetry, *Security Fabric* and *Dashboard* GUI pages cannot be displayed.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.
594416	Accessing FortiGate GUI through SSL VPN web mode causes *Network* > *Interfaces* page to return an error.

Switch Controller

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

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
578031	FortiManager Cloud cannot be removed once the FortiGate has trouble on contract.
600032	SNMP does not provide routing table for non-management VDOM.
623501	FG-80D may fail to boot due to a limitation in the size of the bootloader and kernel.

User & Device

Bug ID	Description
591461	FortiGate does not send user IP to TACACS server during authentication.

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 master to slave during configuration restore.
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.
613730	Unable to update routing table for a resource group in a different subscription with FortiGate Azure SDN.

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.