FortiOS - Release Notes

Version 6.2.3

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

January 9, 2020
FortiOS 6.2.3 Release Notes
01-623-597145-20200109

TABLE OF CONTENTS

Change Log **6**
Introduction and supported models **7**
Supported models 7
Special branch supported models 7
Special notices **9**
New Fortinet cloud services 9
FortiGuard Security Rating Service 9
Using FortiManager as a FortiGuard server 10
FortiGate hardware limitation 10
CAPWAP traffic offloading 10
FortiClient (Mac OS X) SSL VPN requirements 11
Use of dedicated management interfaces (mgmt1 and mgmt2) 11
NP4lite platforms 11
Tags option removed from GUI 11
Changes in default behavior **12**
Changes in CLI defaults **13**
Upgrade Information **16**
Device detection changes 16
FortiClient Endpoint Telemetry license 17
Fortinet Security Fabric upgrade 17
Minimum version of TLS services automatically changed 17
Downgrading to previous firmware versions 18
Amazon AWS enhanced networking compatibility issue 18
FortiLink access-profile setting 19
FortiGate VM with V-license 19
FortiGate VM firmware 19
Firmware image checksums 20
FortiGuard update-server-location setting 20
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**
Special Notices 27
New Features or Enhancements 27
Changes in CLI 28
Changes in Default Value 28
Anti Virus 29

Data Leak Prevention 29
DNS Filter 29
Explicit Proxy 29
Firewall 30
FortiView 30
GUI 30
HA 32
Intrusion Prevention 33
IPsec VPN 33
Log & Report 34
Proxy 34
REST API 35
Routing 35
Security Fabric 36
SSL VPN 36
Switch Controller 37
System 38
Upgrade 39
User & Device 39
VM 40
VoIP 41
Web Filter 41
WiFi Controller 41
Common Vulnerabilities and Exposures 41
Known issues 43
Anti Virus 43
Data Leak Prevention 43
FortiView 43
GUI 43
HA 44
Intrusion Prevention 44
IPsec VPN 44
Log & Report 45
Proxy 45
REST API 45
Routing 45
Security Fabric 46
SSL VPN 46
Switch Controller 46
System 46
User & Device 47
VM 47
Limitations 48
Citrix XenServer limitations 48

Open source XenServer limitations 48

Change Log

Date	Change Description
2019-12-19	Initial release.
2019-12-19	Updated *Resolved Issues* and *Known Issues*.
2019-12-20	Updated *Changes in CLI defaults*.
2019-12-30	Added 585122 to *Resolved Issues*.
2020-01-02	Updated *Product integration and support* > *FortiExtender*.
2020-01-03	Updated *Known Issues*.
2020-01-06	Updated *Introduction and supported models* > *Special branch supported models*. Removed image download note from *Introduction and supported models*.
2020-01-07	Added 581663 to *Resolved Issues*.
2020-01-09	Added FG-60F, FG-61F, FG-100F, and FG-101F to *Introduction and supported models* > *Special branch supported models*.

Introduction and supported models

This guide provides release information for FortiOS 6.2.3 build 1066.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.3 supports the following models.

FortiGate	FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-POE, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, 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-61E
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
FortiOS Carrier	FortiOS Carrier 6.2.3 images are delivered on request and are not available on the Beta portal.

Special branch supported models

The following models are released on a special branch of FortiOS 6.2.3. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1066.

FG-30E-MG	is released on build 8255.
FG-60E-DSL	is released on build 6164.

FG-60E-DSLJ	is released on build 6164.
FG-60F	is released on build 6188.
FG-61F	is released on build 6188.
FG-100F	is released on build 6188.
FG-101F	is released on build 6188.
FG-1100E	is released on build 5401.
FG-1101E	is released on build 5401.
FWF-60E-DSL	is released on build 6164.
FWF-60E-DSLJ	is released on build 6164.

Special notices

- New Fortinet cloud services
- FortiGuard Security Rating Service
- Using FortiManager as a FortiGuard server on page 10
- 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

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 FortinetOne single sign-on (SSO) service. These updates will be available by mid-Q2 2019.

- 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.

Changes in default behavior

CLI

- Removed dependency between `gui-per-policy-disclaimer` in the system setting and `per-policy-disclaimer` in the user setting.
- There is a new default `any-to-any-all-to-all` policy after changing from NGFW mode to policy-based mode.

GUI

- In the *Feature Visibility* page, the *Per-policy Disclaimer* option name was changed to *Policy Disclaimer*.
- *Firewall Policy* was renamed to *SSL Inspection & Authentication* after changing from NGFW mode to policy-based mode.

WiFi Controller

The default extension information setting in `wtp-profile` has changed from disable to enable.

Previous releases	6.2.3 release
config wireless-controller wtp-profile edit <FAP-Profile> set ext-info-enable disable next end	config wireless-controller wtp-profile edit <FAP-Profile> **set ext-info-enable enable <== changed** next end

The default platform type in `wtp-profile` has changed from 220B to 221E.

Previous releases	6.2.3 release
config wireless-controller wtp-profile edit <New profile> config platform set type 220B end next end	config wireless-controller wtp-profile edit <New profile> config platform **set type 221E <== changed** end next end

Changes in CLI defaults

Routing

- `auxiliary session {enable | disable}` option added at the VDOM level.

System

- Consolidate FortiTelemetry and `capwap` into `fabric` to allow Security Fabric access in `system interface`.

Previous releases	6.2.3 release

`config system interface`
`  edit <Port number>`
`  **set allowaccess capwap <== Removed**`
`  **set fortiheartbeat <== Removed**`
`  next`
`end`
	`config system interface`
	`  edit <Port number>`
	`  **set allowaccess fabric <== New**`
	`  next`
	`end`

- Add `execute factoryreset-shutdown` to combine the functionality of the `factory-reset` and `shutdown` commands.
- Add more functions for SMC NTP and the ability to get information from SMC NTP:

```
config system smc-ntp <== New
    set ntpsync disable <== New
    set syncinterval 60 <== New
    set channel 5 <== New
end
```

Web Filter

- Enable `file-filter` password protected blocked for 7Z, RAR, PDF, MSOffice, and MSOfficeX.

Previous releases	6.2.3 release

`config webfilter profile`
`  edit "encrypted-web"`
`  set comment ''`
`  set replacemsg-group ''`
`  unset options`
`  config file-filter`
`  set status enable`
`  set log enable`
`  set scan-archive-contents enable`
`  config entries`
`  edit "1"`
`  set comment ''`
	`config webfilter profile`
	`  edit "encrypted-web"`
	`  set comment ''`
	`  set replacemsg-group ''`
	`  unset options`
	`  config file-filter`
	`  set status enable`
	`  set log enable`
	`  set scan-archive-contents enable`
	`  config entries`
	`  edit "1"`
	`  set comment ''`

Previous releases	6.2.3 release
set protocol http ftp set action log set direction any set password-protected yes **set file-type "zip" <== only zip can be selected** next end end next end	set protocol http ftp set action log set direction any set password-protected yes **set file-type "zip" "7z" "msoffice" "msofficex" "pdf" "rar" <==-changed** next end end next end

WiFi Controller

- FAP-U431F and FAP-U433F can support 802.11ax on 2.4 GHz `radio-2` when the platform mode is `single-5G`.

Previous releases	6.2.3 release
config wireless-controller wtp-profile edit "FAPU431F-default" config platform set type U431F set mode single-5G end config radio-1 set band 802.11ax-5G end config radio-2 set band ? 802.11b 802.11b. 802.11g 802.11g/b. 802.11n 802.11n/g/b at 2.4GHz. 802.11n,g-only 802.11n/g at 2.4GHz. 802.11g-only 802.11g. 802.11n-only 802.11n at 2.4GHz. end config radio-3 set mode monitor end next end	config wireless-controller wtp-profile edit "FAPU431F-default" config platform set type U431F set mode single-5G end config radio-1 set band 802.11ax-5G end config radio-2 set band ? 802.11b 802.11b. 802.11g 802.11g/b. 802.11n 802.11n/g/b at 2.4GHz. **802.11ax 802.11ax/n/g/b at 2.4GHz. <==added** 802.11n,g-only 802.11n/g at 2.4GHz. 802.11g-only 802.11g. 802.11n-only 802.11n at 2.4GHz. **802.11ax,n-only 802.11ax/n at 2.4GHz. <==added** **802.11ax,n,g-only 802.11ax/n/g at 2.4GHz. <==added** **802.11ax-only 802.11ax at**

Previous releases	6.2.3 release
	2.4GHz.<==added end config radio-3 set mode monitor end 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*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Device-based policies – Device type/category and detected devices/device groups can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- Mac-address-based policies – A new address type is introduced (Mac Address Range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

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 6.2.3 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 6.2.3. When the Security Fabric is enabled in FortiOS 6.2.3, all FortiGate devices must be running FortiOS 6.2.3.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.3 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 6.2.3 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 6.2.3 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 6.2.3 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 6.2.3, 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 6.2.3.

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

Product integration and support

The following table lists FortiOS 6.2.3 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 0287 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	• 6.00132
IPS Engine	• 5.00043
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 61 Google Chrome version 68
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 61 Google Chrome version 68
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
OS X El Capitan 10.11.1	Apple Safari version 11 Mozilla Firefox version 61 Google Chrome version 68
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 6.2.3. For inquires about a particular bug, please contact Customer Service & Support.

Special Notices

Bug ID	Description
587666	Mobile token authentication does not work for SSL VPN on SOC3 platforms. Affected models include: FG-60E, FG-60E-POE, FG-61E, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-100E, FG-100EF, FG-101E, FG-140E, FWF-60E, FWF-61E.

New Features or Enhancements

Bug ID	Description

529445	In `wids-profile`, add the new `ap-scan-threshold` setting, which is the minimum signal level of rogue APs detected and required by the managed FortiAP devices. Only the rogue APs with a signal level higher than the threshold will be reported to the FortiGate WiFi Controller.
	`config wireless-controller wids-profile`
	`edit <WIDS-profile-name>`
	`set ap-scan enable`
	`set ap-scan-threshold "-80"`
	`next`
	`end`
	The range of `ap-scan-threshold`, in dBm, is -95 to -20 (default = -90).

557614	FortiGate support for NSX-T v2.4: East/West traffic.
562394	Add support for EMS cloud.
571639	Add support for tracking number of hits to a policy route.
579484	GUI changes in OCVPN to map user workflow habit.
580889	Add vSPU and vNP DPDK port code for FortiGate VMs.
591567	Add support for additional SHA-2 algorithms with SNMPv3.

Changes in CLI

Bug ID	Description

574882	FAP-U431F and FAP-U433F can support 802.11ax on 2.4 GHz `radio-2` when the platform mode is `single-5G`.
	`config wireless-controller wtp-profile`
	`edit "FAPU431F-default"`
	`config platform`
	`set type U431F`
	`set mode single-5G`
	`end`
	`config radio-1`
	`set band 802.11ax-5G`
	`end`
	`config radio-2`
	`set band 802.11ax`
	`end`
	`config radio-3`
	`set mode monitor`
	`end`
	`next`
	`end`

Changes in Default Value

Bug ID	Description

548906	Change default extension information setting in `wtp-profile` from `disable` to `enable`.
	`config wireless-controller wtp-profile`
	`edit <FAP-Profile>`
	`set ext-info-enable enable <== changed`
	`next`
	`end`

585889	Change default platform type setting in `wtp-profile` from `220B` to `221E`.
	`config wireless-controller wtp-profile`
	`edit <New profile>`
	`config platform`
	`set type 221E <== changed`
	`end`
	`next`
	`end`

Anti Virus

Bug ID	Description
590092	Cannot clear `scanunit vdom-stats` to reset the statistics on ATP widget.
590170	Policy in flow mode blocking .JAR archive files.

Data Leak Prevention

Bug ID	Description
586689	Downloading a file with FTP client in EPSV mode will hang.
591676	Enable file filter password protected blocked for 7Z, RAR, PDF, MSOffice, and MSOfficeX.

DNS Filter

Bug ID	Description
561297	DNS filtering does not perform well on the zone transfer when a large DNS zone's AXFR response consists of one or more messages.
563441	7K DNS filter breaking DNS zone transfer.
574980	DNS translation is not working when request is checked against the local FortiGate.
583449	DNS filter explicit block all (wildcard FQDN) not working in 6.2 firmware.
586526	Unable to change DNS filter profile category action after upgrading from 6.0.5 to 6.2.0.

Explicit Proxy

Bug ID	Description
504011	FortiGate does not generate traffic logs for SOCKS proxy.
588211	WAD cannot learn policy if multiple policies use the same FQDN address.
589065	FSSO-based NTLM sessions from explicit proxy do not respect timeout duration and type.
589811	`urfilter` process does not started when adding a category as `dstaddr` in a proxy policy with the deny action.
590942	AV does not forward reply when GET for FTP over HTTP is used.

Firewall

Bug ID	Description
508015	Editing a policy in the GUI changes the FSSO setting to disable.
558996	FortiGate sends type-3 code-1 IP unreachable for VIP.
584451	NGFW default block page partially loads.
585073	Adding too many address objects to a local-in policy causes all blocking to fail.
585122	Recurring and one-time schedules can be renamed to an existing schedule group's name.
590039	Samsung OEM internet browser cannot connect to FortiGate VS/VIP.
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.
597110	When creating a firewall address with the `associated-interface` setting, CMD gets stuck if there is a large nested address group.

FortiView

Bug ID	Description
582341	On *Policies* page, consolidated policies are without names and tooltips; tooltips not working for security policies.

GUI

Bug ID	Description
282160	GUI does not show byte information for aggregate and VLAN interface.
303651	Should hide *Override internal DNS* option if `vdom-dns` is set to `disable`.
438298	When VDOM is enabled, the interface faceplate should only show data for interfaces managed by the admin.
451306	Add a tooltip for IPS *Rate Based Signatures*.
460698	There is no uptime information in the *HA Status* widget for the slave unit's GUI.
467495	A wrong warning message appears that the source interface has no members after enabling an inserted proxy policy.

Bug ID	Description
478472	Options 150, 15, and 51 for the DHCP server should not be shown after removing them and having no related configuration in the backend.
480731	Interface filter gets incorrect result (EMAC VLAN, VLAN ID, etc.) when entries are collapsed.
482437	SD-WAN member number is not correct in *Interfaces* page.
493527	Compliance events GUI page does not load when redirected from the advanced compliance page.
498892	GUI shows wrong relationship between VLAN and physical interface after adding them to a zone.
502962	Get "Fail to retrieve info" for default VDOM link on *Network* > *Interfaces* page.
505066	Not possible to select value for DN field in LDAP GUI browser.
510685	*Hardware Switch* row is shown indicating a number of interfaces but without any interfaces below.
514027	Cannot disable CORS setting on GUI.
531376	Get "Internal Server Error" when editing an aggregate link that has a name with a space in it.
534853	Suggest GUI Interfaces list includes SIT tunnels.
536718	Cannot change MAC address settting when configuring a reserved DHCP client.
537307	"Failed to retrieve info" message appears for `ha-mgmt-interface` in *Network* > *Interfaces*.
538125	Hovering mouse over FortiExtender virtual interface shows incorrect information.
540098	GUI does not display the status for VLAN and loopback in the *Network* > *Interfaces* > *Status* column.
542544	In *Log & Report*, filtering for blank values (*None*) always shows no results.
544442	Virtual IPs page should not show port range dialog box when the protocol is ICMP.
552811	Scripts pushed from FortiCloud do not show up in *System* > *Advanced Settings* when FortiCloud remote access is used.
553290	The tooltip for VLAN interfaces displays as "Failed to retrieve info".
555687	Network mask of a VPN interface is changed to 255.255.255.255 without an actual configuration change.
559866	When sending CSF proxied request, segfault happens (httpsd crashes) if FortiExplorer accesses root FortiGate via the management tunnel.
563053	Warning messages for third-party transceivers were removed in 6.2.1 to prevent excessive RMA or support tickets. In 6.2.2, warnings were re-added for third-party transceivers.
565748	New interface pair consolidated policy added via CLI is not displayed on GUI policy page.
566414	*Application Name* field shows `vuln_id` for custom signature, not its application name in logs.
567369	Cannot save DHCP *Relay* configuration when the *Relay* IP address list is separated by a comma.
573456	FortiGate without disk email alert settings page should remove *Disk usage exceeds* option.

Bug ID	Description
574101	Empty firmware version in managed FortiSwitch from FortiGate GUI.
582658	Email filter page keeps loading and cannot create a new profile when the VDOM admin only has `emailfilter` permission.
583049	Internal server error while trying to create a new interface.
584419	Issue with application and filter overrides.
584426	*Add Selected* button does not show up under *FSSO Fabric Connector* with custom admin profile.
584560	GUI does not have the option to disable the interface when creating a VLAN interface.
586604	No matching IPS signatures are found when *Severity* or *Target* filter is applied.
586749	Enable/disable *Disarm and Reconstruction* in the GUI only affects the SMTP protocol in AV profiles.
587091	When logged in as administrator with web filter read/write only privilege, the *Web Rating Overrides* GUI page cannot load.
588028	If the *Endpoint Control* feature is disabled, the exempt options for captive portal are not shown in the GUI.
588222	*WAN Opt. Monitor* displays *Total Savings* as negative integers during file transfers.
588665	Option to reset statistics from *Monitor* > *WAN Opt. Monitor* in GUI does not clear the counters.
589085	Web filter profile warning message when logged in with read/write admin on VDOM environment.
592244	VIPs dialog page should be able to create VIP with the same extip/extport but different source IP address.
593433	DHCP offset option 2 has to be removed before changing the address range for the DHCP server in the GUI.
594162	Interface hierarchy is not respected in the GUI when a LAG interface belongs to SD-WAN and its VLANs belong to a zone.
594565	Wrong *Sub-Category* appears in the *Edit Web Rating Override* page.

HA

Bug ID	Description
479780	Slave fails to send and receive HA heartbeat when configuring `cfg-revert` setting on FG-2500E.
540632	In HA, `management-ip` that is set on a hardware switch interface does not respond to ping after executing reboot.
575020	HA failing `config sync` on VM01 with error (slave and master have different hdisk status) when master is pre-configured.

Bug ID	Description
581906	HA slave sending out GARP packets in 16-20 seconds after HA monitored interface failed.
585348	`default-gateway` injected by `dynamic-gateway` on PPP interface deleted by other interface down.
585675	`exe backup disk alllogs ftp` command causes FortiGate to enter conserve mode.
586004	Moving VDOM via GUI between virtual clusters causes cluster to go out of sync and VDOM state work/standby does not change.
586835	HA slave unable to get checksum from master. HA sync in `Z` state.
590931	Multiple PPPoE connections on a single interface does not sync PPPoE dynamic assigned IP and cannot start re-negotiation.

Intrusion Prevention

Bug ID	Description
540718	Signal 14 alarm crashes were observed on DFA rebuild.
579018	IPS engine 5.030 signal 14 alarm clock crash at `nturbo_on_event`.
586608	The CPU consumption of ipsengine gets high with customer configuration file.

IPsec VPN

Bug ID	Description
577502	OCVPN cannot register—status "Undefined".
582251	IKEv2 with EAP peer ID authentication validation does not work.
582876	ADVPN connections from the hub disconnects one-by-one and IKE gets stuck.
584982	The customer is unable to log in to VPN with RADIUS intermittently.
589096	In IPsec after HA failover, performance regression and IKESAs is lost.

Log & Report

Bug ID	Description
578057	Action field in traffic log cannot record security policy action—it shows the consolidated policy action.
586038	FortiOS 6.0.6 reports too long VPN tunnel durations in local report.
590598	Log viewer application control cannot show any logs (page is stuck loading).
590852	Log filter can return empty result when there are too many logs, but the filter result is small.
591152	IPS logs set `srcintf(role)`/`dstinf(role)` reversely at the time of IPS signature reverse pattern.
591523	When refreshing logs in GUI, some `log_se` processes are running extremely long and consuming CPU.
593907	Miglogd still uses the daylight savings time after the daylight savings end.
596278	`sentdelta` and `rcvddelta` showing 0 if syslog format is set to CSV.

Proxy

Bug ID	Description
525328	External resource does not support no content length.
549660	WAD crash with signal 11.
573028	WAD crash causing traffic interruption.
579400	High CPU with `authd` process caused by WAD paring multiple line content-encoding error and IPC broken between `wad` and `authd`.
580592	Policy in proxy-based mode with AV and WAF profile denies access to Nginx with enabled gzip compression.
584719	WAD reads `ftp over-limit multi-line` response incorrectly.
587214	WAD crash for `wad_ssl_port_on_ocsp_notify`.
587987	In case of TLS 1.3 with certificate inspection and a certificate with an empty CN name, WAD workers would locate a random size for CN name and then cause unexpected high memory usage in WAD workers.
592153	Potential memory leak that will be triggered by certificate inspection CIC connection in WAD.
593365	WAD crash due to user learned from proxy not purged from the kernel when user is deleted from proxy or zone with empty interface member.
594237	Slow download speed in proxy-based mode compared to flow-based mode.

Bug ID	Description
594725	WAD memory leak detected on `cert_hash in wad_ssl_cert`.
596012	Receive SSL fatal alert with source IP 0.0.0.0.

REST API

Bug ID	Description
587470	REST API to support revision flag.

Routing

Bug ID	Description
371453	OSPF translated type 5 LSA not flushed according to RFC-3101.
524229	SD-WAN `health-check keep` records useless logs under some circumstances.
570686	FortiOS 6.2.1 introduces asymmetric return path on the hub in SD-WAN after the link change due to SLA on the spoke.
582078	ISDB ID is changed after restoring the configuration under the situation where the FortiGate has a previous ISDB version.
584095	SD-WAN option of `set gateway enable`/`set default enable` override available on connected routes.
584477	In transparent mode with asymmetric routing, packet in the reply direction does not use asymmetric route.
585027	There is no indication in `proute` if the SD-WAN service is default or not.
585325	IPv6 route cannot be inactive after `link-monitor` is down when `link-monitor` are set with `ipv4` and `ipv6`.
587198	After failover/recovery of link, E2 route with non-zero forward address recurses to itself as a next hope.
587700	Routing monitor policy view cannot show source and destination data for SD-WAN route and wildcard destination.
587970	SD-WAN rules `route-tag` still used in service rule but not in `diagnose sys virtual-wan-link route-tag-list`.
589620	Link monitor with tunnel as `srcintf` cannot recover after remote server down/up.
592599	FortiGate sends malformed OSPFv3 LSAReq/LSAck packets on interfaces with MTU = 9k.
593864	Routing table is not always updated when BGP gets an update with changed next hop.

Bug ID	Description
594685	Unable to create the IPsec VPN directly in *Network* > *SD-WAN*.
595937	PPPoE interface bandwidth is mistakenly calculated as 0 in SD-WAN.

Security Fabric

Bug ID	Description
575495	FGCP dynamic objects are not populated in the slave unit.
586587	Security Fabric widget keeps loading when FortiSwitches are in a loop, or the FortiSwitch is in MCLAG mode.
587758	Invalid CIDR format shows as valid by the Security Fabric threat feed.
588262	IP address *Threat Feed* fabric connector not working.
589503	*Threat Feeds* show the URL is invalid if there is a special character in the URL.

SSL VPN

Bug ID	Description
525342	In some special cases, SSL VPN main state machine reads function pointer is empty that will cause SSL VPN daemon crash.
556657	Internal website not working through SSL VPN web mode.
557806	Cannot fully load a website through SSL VPN bookmark.
570171	When accessing ACT application through SSL VPN web mode, the embedded calendar request gets wrong response and redirects to login page.
573787	SSL VPN web mode not displaying custom web application's JavaScript parts.
576288	FSSO groups set in rule with SSL VPN interface.
578908	Fails to load bookmark site over SSL VPN portal.
580377	Unable to access https://outlook.office365.com as bookmark in SSL VPN web mode.
582265	RDP sessions are terminated (disconnect) unexpectedly.
583339	Support HSTS `include SubDomains` and `preload` option under SSL VPN settings.
584780	When the SSL VPN portal theme is set to red, the style is lost in the SSL VPN portal.
585754	A VPN SSL bookmark failed to load the Proxmox GUI interface.

Bug ID	Description
586032	Unable to download report from an internal server via SSL VPN web mode connection.
586035	The policy "`script-src 'self'`" will block the SSL VPN proxy URL.
587075	SAML login is not stable for SSL VPN, it requires restarting `sslvpnd` to enable the function.
588066	SSO for HTTPS fails when using "\" (backslash) with the domain\username format.
588119	There is no OS support for the latest macOS Catalina version (10.15) when using SSL VPN tunnel mode.
588587	Different portals of SIPLAN COMPESA do not show properly in web mode.
588720	SSL VPN web portal bookmarks cannot resolve `hostname`.
589015	SSO does not correctly URL-encode POST-ed credentials.
590643	`href` rewrite has some issues with the customer's JS file.
591613	https://outlook.office365.com cannot be accessed in SSLVPN web portal.
592318	After `sslvpn proxy`, some Kurim JS files run with an error.
592935	sslvpnd crashed on FortiGate.
593082	SSL VPN bookmark does not load Google Maps on internal server.
593641	Cannot access HTTPS bookmark, get a blank page.
593850	SSL VPN logs out after some users click through the remote application.
594160	Screen shot feature is not working though SSL VPN portal.
594247	Cannot access https://cdn.i-ready.com through SSL VPN web portal.
595920	SSL VPN web mode goes to 99% on a specific bookmark.
596273	sslvpnd worker process crashes, causing a zombie tunnel session.
596843	Internal website not working in SSL VPN web mode.
597282	The latest FortiOS GUI does not render when accessing it by the SSL VPN portal.

Switch Controller

Bug ID	Description
581370	FortiSwitch managed by FortiGate not updating the RADIUS settings and user group in the FortiSwitch.
586299	Adding factory-reset device to HA fails with `switch-controller.qos` settings in root.
592111	FortiSwitch shows offline CAPWAP response packet getting dropped/failed after upgrading from 6.2.2.

System

Bug ID	Description
484749	TCP traffic with `tcp_ecn` tag cannot go through `ipip ipv6 tunnel` with NP6 offload enabled.
502387	X.509 certificate support required for FGFM portocol.
511790	Router info does not update after plugging out/plugging in USB modem.
528052	FortiGuard filtering services show as unavailable for read-only admin.
547712	HPE does not protect against DDoS attacks like flood on IKE and BGP destination ports.
556408	Aggregate link does not work for LACP mode active for FG-60E internal ports but works for wan1 and wan2 combination.
570759	RX/TX counters for VLAN interfaces based on LACP interface are 0.
572003	There was a hardware defect in an earlier revision of SSD used for FG-61E. When powering off then powering on in a very short time, the SSD may jump into ROM mode and cannot recover until a power circle.
573090	Making a change to a policy through inline editing is very slow with large table sizes.
573238	Session TTL expiry timer is not reset for VLAN traffic when offloading is enabled.
573973	ASIC offloading sessions sticking to interfaces after SD-WAN SLA interface selection.
577423	FG-80D and FG-92D kernel error in CLI during FortiGate boot up.
578259	FG-3980E VLANs over LAG interface show no TX/RX statistics.
578608	High CPU usage due to dnsproxy process as high at 99%.
581496	FG-201E stops sending out packets and NP6lite is stuck.
581528	SSH/RDP sessions are terminated unexpectedly.
581998	Session clash event log found on FG-6500F when passing a lot of the same source IP ICMP traffic over load-balance VIP.
582520	Enabling offloading drops fragmented packets.
583199	`fgfmsd` crashed with signal 11 when some code accesses a VDOM that has been deleted, but does not check the return value from CMDB query.
583602	Script to purge and re-create a local-in-policy ran against the remote FortiGate directly (in the CLI) is causing auto-update issues.
586301	GUI cannot show default Fortinet logo for replacement messages.
586551	When an SD-WAN member is disabled or VWL is disabled, `snmpwalk` shows "No Such Object available on this agent at this OID" message.
587498	FortiGate sends ICMP type 3 code 3 (port unreachable) for UDP 500 and UDP 520 against vulnerability scan.

Bug ID	Description
587540	Netflow traffic records sent with wrong interface index 0 (`inputint = 0` and `outputint = 0`).
588035	Kernel crashes when sniffing packets on interfaces that are related to EMAC VLAN.
588202	FortiGate returns invalid configuration during FortiManager retrieving configuration.
589027	EMAC VLAN drops traffic when asymmetric roue enabled on internet VDOM.
589234	Local system DNS setting instead of DNS setting acquired from upstream DHCP server was assigned to client under management VDOM.
589517	Dedicated management CPU running on high CPU (soft IRQ).
589978	`alertemail username` length cannot go beyond 35 characters.
590295	OID for the IPsec VPN phase 2 selector only displays the first one on the list.
591466	Cannot change the mask for an existing secondary IP on interfaces.
592787	FortiGate got rebooted automatically due to kernel crash.
593606	`diagnose hardware test suite all` fails due to FortiLink loopback test.
594157	FortiGate accepts invalid configuration from FortiManager.
594499	Communication over PPPoE fails after installing PPPoE configuration from FortiManager.
596180	Constant DHCPD crashes.

Upgrade

Bug ID	Description
586793	Address objects have reference to old firewall policy after upgrading from 6.0.6 > 6.2.x NGFW policies.

User & Device

Bug ID	Description
567831	Local FSSO poller regularly missing logon events.
583745	Wrong categorization of OS from device detection.
586334	Brief connectivity loss on shared service when RDP session is logged in to from local device.
586394	Authentication list entry is not created/updated after changing the client PC with another user in FSSO polling mode.

Bug ID	Description
587293	The session to the SQL database is closed as `timeout` when a new user logs in to terminal server.
587519	fnbamd takes high CPU usage and user not able to authenticate.
592241	Gmail POP3 authentication fails with certificate error since version 6.0.5.
592253	RADIUS state attribute truncated in access request when using third-party MFA (ping ID).
593116	Client PC matching multiple authentication methods (firewall, FSSO, RSSO, WSSO) may not be matched to NGFW policies correctly.

VM

Bug ID	Description
571212	Only one CPU core in AWS is being used for traffic processing.
577653	vMotion tasks cause connections to be dropped as sessions related to vMotion VMs do not appear on the destination VMX.
579708	Should replace GUI option to register to FortiCare from AWS PAYG with link to portal for registration.
582123	EIP does not failover if the master FortiGate is rebooted or stopped from the Alibaba Cloud console.
586954	FGCP cluster member reboots in infinite loop and `hatalk` daemon dumps the core with segmentation fault.
588436	Azure SDN connector unable to connect to Azure Kubneretes integrated with AAD.
589445	VM deployed in ESX platform with VMXNET3 does not show the correct speed and duplex settings.
590140	FG-VM-LENC unable to validate new license.
590149	Azure FortiGate crashing frequently when MLX4 driver RX jumbo.
590253	VLAN not working on FortiGate in a Hyper-V deployment.
590555	Allow PAYG AWS VM to bootstrap the configuration first before acquiring FortiCare license.
590780	Azure FortiGate-VM (BYOL) unable to boot up when loading a lower vCPU license than the instance's vCPU.
591563	Azure autoscale not syncing after upgrading to 6.2.2.
592000	In Alibaba Cloud, multiple VPC route entries fail to switch when HA fails over.
592611	HA not fully failing over when using OCI.
593797	FG-VM64-AWS not responding to ICMP6 request when destination IPv6 address is in the neighbor cache entry.

VoIP

Bug ID	Description
582271	Add support for Cisco IP Phone keepalive packet.

Web Filter

Bug ID	Description
560904	In NGFW mode, *Security Profiles* GUI is missing *Web Rating Overrides* page.
581523	Wrong web filter category when using flow-based inspection.
587120	Administrator logged in with web filter read/write privilege cannot create or edit web filter profiles in the GUI.
593203	Cannot enter a name for a web rating override and save—error message appears when entering the name.

WiFi Controller

Bug ID	Description
520677	When editing a FortiAP profile on the FortiGate web UI, the previously selected SSID group(s) cannot be displayed.
555659	When FortiAP is managed with cross VDOM links, the WiFi client cannot join to SSID when `auto-asic-offload` is enabled.
566054	Errors pop up while creating or editing as SSID.
567011	WPA2-Enterprise SSID should support `acct-all-servers` setting in RADIUS to send accounting messages to all servers.
567933	FortiAP unable to connect to FortiGate via IPsec VPN tunnel with `dtls-policy clear-text`.
572350	FortiOS GUI cannot support FAP-U431F and FAP-U433F profiles.
580169	Captive portal (disclaimer) redirect not working for Android phones.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
568788	FortiOS 6.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2007-6750
576090	FortiOS 6.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2019-17655
581663	FortiOS 6.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2019-9496
582538	FortiOS 6.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2019-17656

Known issues

The following issues have been identified in version 6.2.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
563250	Shared memory does not empty out properly under /tmp.

Data Leak Prevention

Bug ID	Description
591178	WAD fails to determine the correct file name when downloading a file from Nextcloud.

FortiView

Bug ID	Description
592309	FortiView physical topology page cannot load; get "Failed to get FortiView data" error message.
599124	Ban IP under FortiView frequently fails.

GUI

Bug ID	Description
514632	Inconsistent `Refcnt` value in GUI when using ports in HA `session-sync-dev`.
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).

Bug ID	Description
557786	GUI response is very slow when accessing IPSec-Monitor (api/v2/monitor/vpn/ipsec is taking a long time).
563549	Recurring httpsd crash at `[0x01f17bc0] => /bin/httpsd lh_char_hash (+0x0000).`
579711	Cannot run *Security Rating* due to disk issue (`diagnose security-rating clean` fails).
584939	VPN event logs shows incorrectly when adding two action filters and if the filter action filter contains "-".
599401	FortiGuard quota category details displays *No matching entries found* for local category.
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
588908	FG-3400E `hasync` reports the "Network is unreachable".
596551	Syncing problem after restoring one VDOM configuration.
598937	Local user creation causes HA to be out of sync for several minutes.

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.

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`.
594962	IPsec VPN IKEv2 interoperability issue when the FortiGate uses a group as P2 selectors with a non-FortiGate in a remote peer gateway.

Log & Report

Bug ID	Description
589782	IPS sensor `log-attack-context` output truncated.
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.
597494	In FIPS-CC mode, API access check returns 401 causing FortiAnalyzer to repeat the login (should return 403).

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.

REST API

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

Routing

Bug ID	Description
600995	Policy routes with large address groups containing FQDNs no longer work after upgrading to 6.2.2.

Security Fabric

Bug ID	Description
599195	Unable to get consistent results from the security rating.
599474	FortiGate SDN connector not seeing all available tag name-value pairs.
600336	Topology does not load and downstream device is stuck connecting in the CSF GUI settings.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.
563022	SSL VPN LDAP group object matching only matches the first policy; is not consistent with normal firewall policy.
594416	Accessing FortiGate GUI through SSL VPN web mode causes *Network* > *Interfaces* page to return an error.
595627	Cannot access some specific sites through SSL VPN web mode.
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.

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.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.

Bug ID	Description
555616	TCP packets send wrong interface and high CPU.
563276	High memory usage on FortiGate 30E after upgrading firmware to 6.0.5.
576337	SNMP polling stopped when FortiManager API script executed onto FortiGate.
578031	FortiManager Cloud cannot be removed once the FortiGate has trouble on contract.
589079	QSFP interface goes down when the `get system interface transceiver` command is interrupted.
594865	`diagnose internet-service match` does not return the IP value of the IP reputation database object.
594871	Potential memory leak triggered by FTP command in WAD.
595338	Unable to execute `ping6` when configuring `execute ping6-options tos`, except for `default`.
595467	Invalid multicast policy created after transparent VDOM restored.

User & Device

Bug ID	Description
573317	SSO admin with a user name over 35 characters cannot log in after the first login.
596844	Admin GUI login makes the FortiGate unstable when there are lots of devices detected by device identification.

VM

Bug ID	Description
575346	`gui-wanopt` cache missing under system settings after upgrading a FortiGate VM with two disks.
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.
596745	In an HA A-P cluster deployed on Azure, the certificate went missing on the slave.
597003	Unable to bypass self-signed certificates on Chrome in macOS Catalina.
598891	FortiGate randomly restarts.
600077	Randomly getting the "vmxnet3 tx:hang" error, which shuts down port2.
601357	FortiGate VM Azure in HA has unsuccessful failover.

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.