FortiOS - Release Notes

Version 6.2.1

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

July 23, 2019
FortiOS 6.2.1 Release Notes
01-621-550798-20190723

TABLE OF CONTENTS

Change Log **5**
Introduction and supported models **6**
Supported models 6
Special branch supported models 6
Special Notices **7**
Common vulnerabilities and exposures 7
New Fortinet cloud services 7
FortiGuard Security Rating Service 7
FortiGate hardware limitation 8
CAPWAP traffic offloading 8
FortiClient (Mac OS X) SSL VPN requirements 9
Use of dedicated management interfaces (mgmt1 and mgmt2) 9
NP4lite platforms 9
Tags option removed from GUI 9
Changes in default behavior **10**
Changes in CLI defaults **14**
Changes in default values **23**
Upgrade Information **26**
Device detection changes 26
FortiClient Endpoint Telemetry license 27
Fortinet Security Fabric upgrade 27
Minimum version of TLS services automatically changed 27
Downgrading to previous firmware versions 28
Amazon AWS enhanced networking compatibility issue 28
FortiLink access-profile setting 28
FortiGate VM with V-license 29
FortiGate VM firmware 29
Firmware image checksums 30
FortiGuard update-server-location setting 30
FortiView widgets 30
Product Integration and Support **31**
Language support 33
SSL VPN support 33
SSL VPN standalone client 33
SSL VPN web mode 34
SSL VPN host compatibility list 34
Resolved Issues **36**
Known Issues **47**
Limitations **51**
Citrix XenServer limitations 51

Open source XenServer limitations 51

Change Log

Date	Change Description
2019-07-18	Initial release.
2019-07-23	Added FG-VM64-RAXONDEMAND to Introduction and supported models on page 6.

Introduction and supported models

This guide provides release information for FortiOS 6.2.1 build 0932.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.1 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-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
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, 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 6.2.1 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 6.2.1. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0932.

FG-VM64-AZURE	is released on build 5163.
FG-VM64-AZUREONDEMAND	is released on build 5163.

Special Notices

- Common vulnerabilities and exposures
- New Fortinet cloud services
- FortiGuard Security Rating Service
- FortiGate hardware limitation
- CAPWAP traffic offloading
- FortiClient (Mac OS X) SSL VPN requirements
- Use of dedicated management interfaces (mgmt1 and mgmt2)
- NP4lite platforms

Common vulnerabilities and exposures

FortiOS 6.2.1 is no longer vulnerable to the issue described in the following link - https://fortiguard.com/psirt/FG-IR-19-144.

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-2R
- FWF-50E
- FWF-51E

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

Firewall

Remove dependency of `ssl-ssh-profile` on `utm-status` under firewall policy (531885).

Previous releases	6.2.1 release
You must enable `utm-status` under firewall policy before configuring `ssl-ssh-profile`.	You can configure `ssl-ssh-profile` by itself. When you upgrade, this configuration is added to the existing firewall policy.

Log & Report

Starting from the 6.2.1 release, `exe log list` displays the result of the current log device.

Previous releases	6.2.1 release
`exe log list` only lists the disk log file.	`exe log list` lists the log file from the current log device (disk/memory). `exe log list` shows the memory log file in `exe log filter device memory`. `exe log list` shows the disk log file in `exe log filter device disk`.

Separate policy and address `log-uuid` options into two individual options.

Previous releases	6.2.1 release

`config system global`
`  set log-uuid [policy-only | extended | disable]`
`end`
	`config system global`
	`  set log-uuid-policy [enable | disable]`
	`  set log-uuid-address [enable | disable]`
	`end`

System

Starting from the 6.2.1 release, Global admin can only back up but not restore the configuration file.

Previous releases	6.2.1 release
Super admin: can back up and restore configuration file. Global admin: **can back up and restore configuration file**.	Super admin: can back up and restore configuration file. Global admin: **can only back up configuration file**. VDOM admin: can back up and restore VDOM configuration file with full Admin and Maintenance permission.

Previous releases	6.2.1 release
VDOM admin: can back up and restore VDOM configuration file with full Admin and Maintenance permission.	

Devices configured under `security-exempt-list` are void after upgrading to 6.2.1.

FortiOS 6.2.1 removes any use of device enforcement from various FortiGate features.

Previous releases	6.2.1 release
config user device-category <==removed **config user device-access-list <==removed** **config user device-group <==removed** config user security-exempt-list edit [List Name] config rule edit [Rule ID] **set devices [Device or group name] <==removed** set srcaddr [Address or group name] next end next end config system interface edit [Interface] set ip [IP address and subnet mask] **set device-access-list [Access list name] <==removed** **set device-identification-active-scan [enable | disable] <==removed** next end config firewall policy edit [Policy ID] set name [Policy name] **set device [Device or group name] <==removed** next end config firewall policy6 edit [Policy ID] set name [Policy name]	config user security-exempt-list edit [List Name] config rule edit [Rule ID] set srcaddr [Address or group name] next end next end config system interface edit [Interface] set ip [IP address and subnet mask] next end config firewall policy edit [Policy ID] set name [Policy name] next end config firewall policy6 edit [Policy ID] set name [Policy name] next end

Previous releases	6.2.1 release
set device [Device or group name] <==removed next end	

WiFi Controller

The VAP schedule is changed from accepting only a recurring schedule to accepting all types of firewall schedule: recurring schedule, one-time schedule, and schedule group.

Previous releases	6.2.1 release
	config wireless-controller vap edit "wifi-t-1" **set schedule "group1"** next end

The LED schedule is changed from accepting only a recurring schedule to accepting all types of firewall schedule: recurring schedule, one-time schedule, and schedule group.

Previous releases	6.2.1 release
	config wireless-controller wtp-profile edit "FAP321C-default" **set led-schedules "group1"** next end

The `ble-profile` setting in `wtp-profile` is now configurable for the FAP-321E platform.

Previous releases	6.2.1 release
	config wireless-controller wtp-profile edit "FAP321E-default" config platform set type 321E end **set ble-profile "BLE-full" <==configurable** set handoff-sta-thresh 55 config radio-1 set band 802.11n,g-only end config radio-2

Previous releases	6.2.1 release
	set band 802.11ac end next end

Changes in CLI defaults

Anti-Spam

Rename `spamfilter` to `emailfilter`.

Previous releases	6.2.1 release

`config` **`spamfilter`** `bwl`
`end`
 	
`config` **`spamfilter`** `profile`
`end`
 	
`config firewall policy`
`edit [Policy ID]`
`set` **`spamfilter-profile`** `[Profile Name]`
`next`
`end`
	`config` **`emailfilter`** `bwl`
	`end`
	
	`config` **`emailfilter`** `profile`
	`end`
	
	`config firewall policy`
	`edit [Policy ID]`
	`set` **`emailfilter-profile`** `[Profile Name]`
	`next`
	`end`

Data Leak Prevention

Rename DLP `fp-sensitivity` to `sensitivity`.

Previous releases	6.2.1 release
`config dlp` **`fp-sensitivity`** `end`	`config dlp` **`sensitivity`** `end`

Firewall

Rename `utm-inspection-mode` to `inspection-mode` under firewall policy.

Previous releases	6.2.1 release

`config firewall policy`
`edit [Policy ID]`
`set` **`utm-inspection-mode`** `[proxy | flow]`
`next`
`end`
	`config firewall policy`
	`edit [Policy ID]`
	`set` **`inspection-mode`** `[proxy | flow]`
	`next`
	`end`

Add a new direction command to Internet service group. Members are filtered according to the direction selected. The direction of a group cannot be changed after it is set.

Previous releases	6.2.1 release
config firewall internet-service-group edit [Internet Service Group Name] set member 65537 65538 next end	config firewall internet-service-group edit [Internet Service Group Name] **set direction [source | destination | both]** set member 65537 65538 next end

FortiView

The following FortiView CLI has been changed in this release.

Previous releases	6.2.1 release
config system admin edit [User Name] config gui edit [Dashboard ID] config widget edit [Widget ID] set type fortiview **set report-by source <==removed** **set timeframe realtime <==removed** **set sort-by "bytes" <==removed** **set visualization table <==removed** next end next end next end	config system admin edit [User Name] config gui edit [Dashboard ID] config widget edit [Widget ID] set type fortiview **set fortiview-type '' <==added** **set fortiview-sort-by '' <==added** **set fortiview-timeframe '' <==added** **set fortiview-visualization '' <==added** **set fortiview-device '' <==added** next end next end next end

HA

The CLI command for HA member management is changed.

Previous releases	6.2.1 release
execute ha manage [ID]	execute ha manage [ID] **[admin-username]**

Intrusion Prevention

Move Botnet configuration option from interface level and policy level to IPS profile.

Previous releases	6.2.1 release
config system interface edit [Interface Name] **set scan-botnet-connections [disable | block | monitor]** next end config firewall policy edit [Policy ID] **set scan-botnet-connections [disable | block | monitor]** next end config firewall proxy-policy edit [Policy ID] **set scan-botnet-connections [disable | block | monitor]** next end config firewall interface-policy edit [Policy ID] **set scan-botnet-connections [disable | block | monitor]** next end config firewall sniffer edit [Policy ID] **set scan-botnet-connections [disable | block | monitor]** next end	config ips sensor edit [Sensor name] **set scan-botnet-connections [disable | block | monitor]** next end

IPsec VPN

Add `net-device` option under static/DDNS tunnel configuration.

Previous releases	6.2.1 release
config vpn ipsec phase1-interface edit [Tunnel Name] set type [static | ddns] next end	config vpn ipsec phase1-interface edit [Tunnel Name] set type [static | ddns] **set net-device [enable | disable]** next end

Log & Report

Move `botnet-connection` detection from malware to `log threat-weight`.

Previous releases	6.2.1 release
config log threat-weight config malware **set botnet-connection [critical | high | medium | low | disable]** end end	config log threat-weight **set botnet-connection [critical | high | medium | low | disable]** end

SDS.

Previous releases	6.2.1 release
config log threat-weight config malware **set botnet-connection [critical | high | medium | low | disable]** end end	config log threat-weight **set botnet-connection [critical | high | medium | low | disable]** end

Add new certificate verification option under FortiAnalyzer setting.

Previous releases	6.2.1 release
config log fortianalyzer setting set status enable set server [FortiAnalyzer IP address] end	config log fortianalyzer setting set status enable set server [FortiAnalyzer IP address] **set certificate-verification [enable | disable]** **set serial [FortiAnalyzer Serial number]** **set access-config [enable | disable]** end

Proxy

Move SSH redirect option from firewall `ssl-ssh-profile` to firewall policy.

Previous releases	6.2.1 release

config firewall ssl-ssh-profile
  edit [Profile Name]
  config ssh
  set ssh-policy-check [enable | disable]
  end
  next
end
	config firewall policy
	 edit [Policy ID]
	  set ssh-policy-redirect [enable | disable]
	 next
	end

Move HTTP redirect option from profile protocol option to firewall policy.

Previous releases	6.2.1 release

config firewall profile-protocol-option
  edit [Profile Name]
  config http
  set http-policy [enable | disable]
  end
  next
end
	config firewall policy
	 edit [Policy ID]
	  set http-policy-redirect [enable | disable]
	 next
	end

Move UTM inspection mode from VDOM setting/AV profile/webfilter profile/emailfilter profile/DLP sensor to firewall policy.

Previous releases	6.2.1 release

config system setting
  set inspection-mode [proxy | flow]
end
 	
config antivirus profile
  edit [Profile Name]
  set inspection-mode [proxy | flow-based]
  next
end
 	
config webfilter profile
  edit [Profile Name]
  set inspection-mode [proxy | flow-based]
  next
end
	config firewall policy
	  edit [Policy ID]
	  set inspection-mode [flow | proxy]
	  next
	end

Previous releases	6.2.1 release
config spamfilter profile edit [Profile Name] **set flow-based [enable | disable]** next end config dlp sensor edit [Sensor Name] **set flow-based [enable | disable]** next end	

Routing

For compatibility with the API, the CLI command for OSPF MD5 is changed from a single line configuration to sub-table configuration.

Previous releases	6.2.1 release
config router ospf config ospf-interface edit [Interface Entry Name] set interface [Interface] set authentication md5 **set md5-key [Key ID] [Key String Value]** next end end	config router ospf config ospf-interface edit [Interface Entry Name] set interface [Interface] set authentication md5 **config md5-keys** **edit [Key ID]** **set key-string [Key String Value]** **next** **end** next end end

The name `internet-service-ctrl` and `internet-service-ctrl-group` is changed to `internet-service-app-ctrl` and `internet-service-app-ctrl-group` to specify it's using application control.

Previous releases	6.2.1 release
config system virtual-wan-link config service edit [Priority Rule ID] set internet-service enable **set internet-service-ctrl [Application ID]** **set internet-service-ctrl-group [Group Name]** next end end	config system virtual-wan-link config service edit [Priority Rule ID] set internet-service enable **set internet-service-app-ctrl [Application ID]** **set internet-service-app-ctrl-group [Group Name]** next end end

Add cost for each SD-WAN member so that in the SLA mode in a SD-WAN rule, if SLAs are met for each member, the selection is based on the cost.

Previous releases	6.2.1 release
config system virtual-wan-link config member edit [Sequence Number] next end end	config system virtual-wan-link config member edit [Sequence Number] **set cost [Value]** next end end

Add a load-balance mode for SD-WAN rule. When traffic matches this rule, this traffic should be distributed based on the LB algorithm.

Previous releases	6.2.1 release
config system virtual-wan-link config service edit [Priority Rule ID] **set mode [auto | manual | priority | sla]** next end end	config system virtual-wan-link config service edit [Priority Rule ID] **set mode [auto | manual | priority | sla | load-balance]** next end end

Security Fabric

Add control to collect private or public IP address in SDN connectors.

Previous releases	6.2.1 release
config firewall address edit [Address Name] set type dynamic set comment '' set visibility enable set associated-interface '' set sdn aws set filter "tag.Name=publicftp" next end	config firewall address edit [Address Name] set type dynamic set comment '' set visibility enable set associated-interface '' set sdn aws set filter "tag.Name=publicftp" **set sdn-addr-type [private | public | all]** next end

Add generic support for integrating ET products (FortiADC, FortiMail, FortiWeb, FortiDDoS, FortiWLC) with Security Fabric.

Previous releases	6.2.1 release

config system csf
  config fabric-device
  edit [Device Name]
  set device-ip [Device IP]
  set device-type fortimail
  set login [Login Name]
  set password [Login Password]
  next
  end
end
	config system csf
	  config fabric-device
	  edit [Device Name]
	  set device-ip [Device IP]
	  set https-port 443
	  set access-token [Device Access Token]
	  next
	  end
	end

Add support for multiple SDN connectors under dynamic firewall address.

Previous releases	6.2.1 release

config firewall address
  edit [Address Name]
  set type dynamic
  set color 2
  set sdn azure
  set filter "location=NorthEurope"
  next
end
	config firewall address
	  edit [Address Name]
	  set type dynamic
	  set color 2
	  set sdn [SDN connector instance]
	  set filter "location=NorthEurope"
	  next
	end

System

Add split VDOM mode configuration.

Previous releases	6.2.1 release

config global
  set vdom-admin [enable | disable]
end
	config global
	  set vdom-admin [no-vdom | split-vdom | multi-vdom]
	end

WiFi Controller

Option changes for `darrp`.

Previous releases	6.2.1 release
config wireless-controller timers set darrp-optimize 0 **set darrp-day monday <==removed** **set darrp-time "12:00" <==removed** end	config wireless-controller timers **set darrp-optimize-schedules "default-darrp-optimize" <==added** end

Option changes for `wids-profile`.

Previous releases	6.2.1 release
config wireless-controller wids-profile edit "default" **set ap-bgscan-disable-day monday <==removed** **set ap-bgscan-disable-start 00:00 <==removed** **set ap-bgscan-disable-end 23:59 <==removed** next end	config wireless-controller wids-profile edit "default" **set ap-bgscan-disable-schedules "always" <==added** next end

New `wfa-compatibility` command for compatibility with previous WiFi specifications. This command only controls the minimum length of the pre-shared key (PSK) in WPA/WPA2-Personal SSID. When disabled, the PSK must contain 12 or more characters. When enabled, the PSK must contain eight or more characters. The default is disable for security enforcement.

Previous releases	6.2.1 release
	config wireless-controller setting **set wfa-compatibility [enable | disable]** end

New command to enable or disable multi-user `MIMO` on "Wave 2" 802.11ac FAP units managed by FortiGate. The default is enable.

Previous releases	6.2.1 release
	config wireless-controller vap edit [VAP Name] **set mu-mimo [enable | disable]** next end

Changes in default values

Firewall

The default profile for `ssl-ssh-profile` is changed from `certificate-inspection` to `no-inspection`.

Previous releases	6.2.1 release

Config firewall policy
  edit [Policy ID]
  set ssl-ssh-profile **certificate-inspection**
  next
end
	Config firewall policy
	  edit [Policy ID]
	  set ssl-ssh-profile **no-inspection**
	  next
	end

IPsec VPN

The default value for `net-device` option under dynamic(dialup) tunnel has changed from `disable` to `enable`.

Previous releases	6.2.1 release

config vpn ipsec phase1-interface
  edit [Tunnel Name]
  set type dynamic
  set net-device **disable**
  next
end
	config vpn ipsec phase1-interface
	  edit [Tunnel Name]
	  set type dynamic
	  set net-device **enable**
	  next
	end

Log & Report

The default value, minimum value, and maximum value for memory log is changed.

Previous releases	6.2.1 release

config log memory global-setting
  set max-size **65536**
end
	config log memory global-setting
	  set max-size [**1% of total RAM**]
	end

Routing

The default SD-WAN `health-check` interval is changed from `1` to `500` and the unit is changed from `seconds` to `milliseconds`.

Previous releases	6.2.1 release
config system virtual-wan-link config health-check edit [Health Check Name] set interval **1** next end end	config system virtual-wan-link config health-check edit [Health Check Name] set interval **500** next end end

The default `link-monitor` interval is changed from `1` to `500` and the unit is changed from `seconds` to `milliseconds`.

Previous releases	6.2.1 release
config system link-monitor edit [Link Monitor Name] set interval **1** next end	config system link-monitor edit [Link Monitor Name] set interval **500** next end

System

The default protocol used for FortiGuard service communication is changed from UDP to HTTPS.

The protocol setting remains unchanged for FortiGates upgrading from v6.0 to v6.2.

Previous releases	6.2.1 release
config system fortiguard set protocol **udp** set port 8888 end	config system fortiguard set protocol **https** set port 8888 end

Switch Controller

The default value for FortiLink split interface is changed from `disable` to `enable`.

Previous releases	6.2.1 release

`config system interface`
`  edit [FortiLink Interface]`
`  set fortilink enable`
`  set fortilink-split-interface` **`disable`**
`  next`
`end`
	`config system interface`
	`  edit [FortiLink Interface]`
	`  set fortilink enable`
	`  set fortilink-split-interface` **`enable`**
	`  next`
	`end`

WiFi Controller

The default `darrp` interval is changed from 1800(s) to 86400(s).

Previous releases	6.2.1 release

`config wireless-controller timers`
`  set darrp-optimize 1800`
`end`
	`config wireless-controller timers`
	`  set darrp-optimize` **`86400`**
	`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.
- Mac-address-based device policies – Detected devices 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 6.2.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.2.0
- FortiClient EMS 6.2.0
- FortiClient 6.2.0
- 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 Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.1. When Security Fabric is enabled in FortiOS 6.2.1, all FortiGate devices must be running FortiOS 6.2.1.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.1 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 6.2.1 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 older AWS VM versions. After downgrading a 6.2.1 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.2.1 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

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 6.2.1, 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 6.2.1.

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

Product Integration and Support

The following table lists FortiOS 6.2.1 product integration and support information:

Web Browsers	• Microsoft Edge 41 • Mozilla Firefox version 59 • Google Chrome version 65 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 41 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 59 • Google Chrome version 65 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 27. 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 27. 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 27 and Fortinet Security Fabric upgrade on page 27. 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 0278 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8

FortiExtender	• 3.2.1
AV Engine	• 6.00132
IPS Engine	• 5.00021
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 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, and 6.5
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 6.2.1. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
528743	Copy/paste of IPv4 policy does not work once AV profile is applied.
557259	FortiGates using AV-Profile proxy mode with `servercomfort` options enabled sending same request twice to the server.

Data Leak Prevention

Bug ID	Description
540903	Missed filename in the office365_Attachment. Download DLP log while it is blocked\Allowed.
547437	WAD crash due to scheduler error occurs when oversized file is bypassing the DLP sensor.
548396	DLP archiving intermittently blocks a file when it should be log only.

DNS Filter

Bug ID	Description
505474	DNS events are not included in the *security event list*.
525068	No need to resolve safe search FQDN if not used.

Endpoint Control

Bug ID	Description
521645	Traffic blocked after enabling *Compliance* on SSL VPN interface.
554765	Revert IPv6 `src-spoof` for GTP.

Explicit Proxy

Bug ID	Description
545724	FortiGate cannot upload file to FortiSandbox when AV profile added in only Proxy-policy.
548415	User cannot pass authentication after timeout if using IP-based authentication.

Firewall

Bug ID	Description
474239	Some DCE-RPC mapped connections are intermittently blocked by policy 0.
521913	Session timers don't update for VLAN traffic over VWP.
524599	Sessions TTL expire timer is not reset when traffic goes through if traffic is offloaded in a TP VDOM.
537349	VIP with central NAT does not hide real IP.
539530	Firewall-session-dirty check-new is blocking traffic and causing session spike.
543469	Cannot create VIP6 range over 31 bits.
546953	DNS Filter column and Profile Group column is missing on policy list.
551747	Not able to configure VIP from GUI with port forwarding for the same TCP and UDP port.
555992	Changes to per-IP shaper settings not reflected in offloaded sessions.
560617	FortiGate logging is not stable: failed-log and log-in-queue.

FortiView

Bug ID	Description
538873	Traffic shaper info missing under Shaper column in FortiView.
539981	Unable to see Source DNS Name in FortiView.

GUI

Bug ID	Description
504770	Introduce an enable/disable button in the GUI to toggle central SNAT table.
532309	Custom device page keep loading and cannot create device group.
537550	HTTPSD uses high CPU when accessing GUI network interfaces.
545074	Unable to login into FortiGate GUI with Yubikey. CLI works as expected.
546254	Forward traffic log cannot be shown on Windows Edge browser.
547393	GUI still shows `fortianalyzer-cloud` connection status error even after FortiGate connects to `fortianalyzer-cloud`.
547458	Cannot access VOIP profile list and only the default profile editor is shown.
547808	Security rating event logs cannot be shown in `split-vdom` FortiGate GUI.
548091	Cannot configure network interface IP addresses from GUI for FG-5001D and FG-5001E.
552329	NP6 sessions dropped after any change in GUI.

HA

Bug ID	Description
501200	Requirement for disabling IPsec SA and IKE SA in FGSP cluster-sync solution.
519266	FGT-HA does not fail over when pingserver is down the second time.
538512	`ha-direct` option for OCSP.
543724	After restoring configuration, FortiGate added unexpected parameters that are not set.
545371	Being Dual Master in specific situation if two `pingsvr` is set.
546714	GARP is output even though GARP setting is disabled.
547367	Cannot synchronize slave from scratch in v6.0.4 with 500 VDOMs, duplicate global profiles.
547700	HA out of sync after upgraded in multi-VDOM environment.
548695	FortiGate master not sending all system events.
549969	After upgrade to special build 5.6.7 b3638, cluster is out of sync when a new guest user is created.
549991	`fgLinkMonitorState` is not accurate.
553231	Moving VDOM between virtual clusters causes cluster to go out of sync.
556057	FGSP cluster members showing out of sync with four members.

ICAP

Bug ID	Description
541423	After any configuration change is applied to FortiGate device, the Symantec ICAP server rejects connections due to too many connections.
551488	FortiGate not sending blocked content page received from the ICAP server to the client.

Intrusion Prevention

Bug ID	Description
528860	IPS archive PCAP periodically cannot capture.
546399	FortiOS runs to conserve mode because IPS engine is taking a lot of memory (memory leak in heap).
548649	IPS custom signature is not detected after FortiGate is rebooted or upgraded.
548908	SSL mirroring does not work on VLAN interface with NTURBO enabled.
552168	IPS archive PCAP usage cannot clear by deleting IPS log and actual PCAP files.
553262	TCP connections through IPsec (bound to loopback) do not work when IPS offload is enabled to NTurbo.
556538	Enabling IPS on IPv4 policy impacting HTTPS traffic over the site to site VPN using PPOE for internal servers.

IPsec VPN

Bug ID	Description
474870	Source MAC address is not updated for offloaded IPsec sessions.
481201	The OCVPN feature is delayed about one day after registering on FortiCare.
518681	`npu-offload` enabled and failover occurred on the checkpoint firewall (upstream firewall) the tunnel is up but traffic is not passing.
534444	Unable to delete IPsec VPN tunnel phase-1 interface config even though we do not have any reference.
542169	Dialup IPsec "net-device" should continue to default to "disable" in 6.2.
545871	IPsec tunnel can't establish if OCVPN members with different Fortinet_CA and Fortinet_factory cert.
546212	Multiple ADVPN shortcuts should be allowed between two spokes.
546459	IKE route overlap should be allowed across two distinct dialup phase1 with 'net-device disable'.
547062	After VDOM config restore, routes are active for IPsec tunnels that are not active.
547293	OSPF point-to-multipoint re-convergence with dailup IPsec.
548032	IKEv2 tunnel does not establish to Google VPN Gateway because of Identification Payload mismatch.

Log & Report

Bug ID	Description
545322	Send interface information to FortiAnalyzer using `miglogd`.
551031	FortiGate lost logs to FortiAnalyzer when route is changed and without physical interface down.

Proxy

Bug ID	Description
513470	WAD crashes on `wad_http_client_notify_scan_result.isra.XXX`.
522827	Add GUI support for `unsupported-ssl` option in SSL inspection profile.
542189	AV profile in proxy mode, with inspect-all enabled, causes timeout when accessing some sites.
544517	WAD process crashing and affecting HTTP/HTTPS traffic.
546360	When applying proxy address in transparent proxy policy, FortiGate blocks traffic and reports `SSL_ERROR_SYSCALL`.
548233	SMTP, POP3, IMAP `starttls` cannot be exempted by FortiGate when first time traffic goes through FortiGate.
549295	WAD crash causes high CPU usage.

Bug ID	Description
549660	WAD crashes with signal 11.
549787	Unable to fetch the Root and Intermediate Certificate.
550895	FG-1500D goes into kernel conserve mode. WAD process consuming high memory.

REST API

Bug ID	Description
541246	Segmentation Fault when generating VPN certificate via REST API.

Routing

Bug ID	Description
503686	Application PDMD crashes.
528145	BGP Configuration gets applied to the wrong VDOM if user switches VDOM selection in between operations (slow GUI).
529512	SSL VPN user gets disconnected when load-balance-mode is measured-volume-based in SD-WAN.
535055	When adding more than seven VPN tunnels to SD-WAN, PPOE default routes disappear.
537054	IPsec interface Internet service router can't work normally.
540682	SD-WAN sends traffic to interfaces with volume-ratio set to 0.
546198	SD-WAN performance SLA via GRE-Tunnel fails to set options or connect ping6 socket for monitor.
549958	Kernel panic due to deletion of ECMp session.
550342	Since upgrade to 6.2, getting RADVD IPv6 router advertisement logs, although IPv6 is not configured on receiving interface.
551492	BGP neighbors are lost on configuration change (large configuration file).
552350	BFD peers down, not seen (over BGP up).
554077	OSPF MD5 authentication issues after upgrade to 6.2.0.
558689	Traffic dropped by anti-replay in ECMP with IPS.
558690	Session timer left at half-open value once established in an ECMP with IPS context.
559146	When a route is evaluated with multiple match conditions including route tag in a route map, route tag is evaluated.
559149	Wrong protocol and sport shown for SD-WAN and regular policy routes.
561097	SD-WAN rule corrupted upon reboot after ISDB update.

Security Fabric

Bug ID	Description
525572	Security Fabric topology page always shows FortiGate HA slave has incompatible firmware version.
547509	Fail to configure Security Fabric if only enable FortiAnalyzer cloud logging not FortiAnalyzer logging in GUI.
547659	Access denied error when reviewing security recommendations from physical topology in VDOM mode.
557821	IP threat feed won't work.

SSL VPN

Bug ID	Description
489110	SSL VPN web-mode fails to access Angular 5 application.
509333	SSL VPN to Nextcloud doesn't open.
513572	FortiGate not sending Framed-IP-Address attribute to for SSL VPN tunnel in RADIUS accounting packet.
515158	SSL VPN web portal login FGT6.0.3 B0191 admin gets blank page.
522571	LAG interface not available for SSL VPN listening interface.
527476	Update from web mode fails for SharePoint page using MS NLB.
539207	Unable to get to *http://spiceworks.int.efwnow.com:9750/tickets/v2#open_tickets* via SSL VPN bookmark.
539719	Signal 11 (segmentation fault) on application `sslvpnd`.
540059	Graylog web application is not working through SSL VPN HTTPS.
540328	SSL VPN web mode accessing internal server getting `ERR_EMPTY_RESPONSE` in browsers.
542480	Internal server script stuck at loading when page accessed over SSL VPN web portal.
542706	With groups and its users in different SSL VPN policies and accessing resources via web, only user based policies are processed.
543091	RDP through SSL VPN web mode will disconnects if copying long text.
545440	The command user-bookmark should not be a prerequisite command for allow-user-access as it also affects Quick Connections.
545810	Subpages on internal websites are not working via SSL VPN web mode.
546161	TX packet drops on ssl.root interface.
546187	SSL VPN login auth times out if primary RADIUS server becomes unavailable.
546280	Internal web site (*confluence.1wa.local*) not loading all elements with SSL VPN web mode (internally it works fine).

Bug ID	Description
546748	Cannot log in to internal server through SSL VPN web mode.
547069	Customer application is displayed wrong through SSL VPN bookmark.
548321	SSL VPN doesn not open QNAP shared folder link.
549588	No *Error: Permission denied* prompt when using the wrong username/password login SSL VPN web with special replacement login page.
549654	Citrix bookmarks should be disabled in SSL VPN portal.
549924	Local resource web interface not loading through SSL VPN web mode.
551535	http 302 redirection is not parsed by SSL VPN proxy (web mode / bookmark).
551923	SSL VPN crashing constantly.
552018	Web mode gets JavaScript errors when accessing internal web site.
553540	Empty RADIUS accounting info supplied for SSL VPN users via `account-interim-interval`.
554378	SSL VPN bookmark sending back to portal home after correct login inside backend application.
554740	Fails to load web pages in SSL VPN web portal.
555983	Internal web portal replies with HTTP *404 Not Found* when accessed via SSL VPN web portal bookmark.
556326	SSL VPN web mode JavaScript error accessing internal resources.
559790	SSL VPN web-mode not performing proxy properly on internal websites.
559932	Customer unable to load website through web-mode SSL VPN.

Switch Controller

Bug ID	Description
548145	Configuring FortiLink from GUI does not work on platforms that do not support hardware switch.
549770	FortiSwitch `export-to` commands do not sync, causing HA sync problem.
555366	VLAN tagging issue to trunk having space in names.

System

Bug ID	Description
493128	`bcm.user` always takes nearly 70% CPU after running Nturbo over IPsec script.
527868	SLBC FortiOS should prevent change of default management VDOM.
529932	Primary DNS server is not queried even after 30 seconds.
533214	After executing shutdown, FGT90E keeps responding to ICMP requests.

Bug ID	Description
534757	Device 80D reboots every 2-3 days with a kernel panic error.
537571	IPS/AV not forwarding return traffic back to clients.
537989	Kernel static route randomly lost.
540634	Status of a port member of a redundant interface changes if an alias is set.
540905	SNMP trap: FortiGate does not generate `fgTrapAvOversizeBlock` and `fgTrapAvOversizePass`.
541527	Changing the order of VDOM in system admin when connected with TACACS+ wildcard admin is not propagated to other blades.
542441	SNMP monitoring of the implicit deny policy not possible.
542482	NTurbo is causing `TX_XPX_QFULL`.
544828	FortiGate 301E consumes high memory even when there's no traffic.
545717	USB Modem Huawei E173u-2 not working on FortiGate 60E device.
546169	DHCPD is using more memory on the slave unit than the active unit.
546746	Cannot lease DHCP address over IPsec for dialup-forticlient users.
547625	Physical interface, part of aggregate interface, disabled with CLI not going down after reboot.
547720	FortiGate does not support DH 1024 bits as SSH server.
547869	LACP member ports exhibit odd behavior regarding admin up and down.
548076	FortiGateCloud cannot restore configuration on FortiGate.
548315	Execute ping does not provide accurate time values.
548443	DHCP enabled interface occasionally fails to perform discovery.
548553	VDOM restore has config loss when interfaces have subnet overlap.
549922	Cannot add description to security zones.
550797	Misleading CLI help left over.
551374	DNSProxy causes the device to go to conserve mode.
551696	Status of a port member of a aggregated interface changes if a member's alias/description is set.
552908	Restoring VDOM configuration removes interfaces from zones.
552935	FortiGate admin access does not offer SSH-RSA when EC Certificate is used for GUI `admin-server-cert`.
554099	Can't poll SNMP v3 statistics for BGP when `ha-direct` is enabled under SNMP user.
555994	Kernel/system memory leak.

Upgrade

Bug ID	Description
546874	Increase firewall.address tablesize for 80-90 series.
548256	Upgrading to v6.2 from v6.0.x causes CIFS/SMB configurations in AV profile to be lost.
548813	Upgrading or downgrading the firmware image using FortiGuard as the source, and as initiated from the *System* > *Firmware* page, fails during download of the firmware image. The page still can be used to view the upgrade path, but as a workaround, you will need to manually download the firmware image from Fortinet's Support site, and then initiate an upgrade or downgrade from the same page under the *Upload Firmware* section.

User & Device

Bug ID	Description
504375	Guest User Print Template doesn't insert the images.
518129	FSSO failover is not graceful.
533838	WAD re-signs valid web sites with Untrusted CA certificate.
534678	`auth-https-port` (1003) for captive portal authentication cannot disable TLS1.1 support.
535488	IP addresses of discovered devices in the device inventory menu are not showing after FortiGate reboots.
538000	FSSO(polling) user names with special character are not showing up in FortiGate.
538218	Mobile Token authentication fails in vCluster on physical slave.
538666	FortiToken assignment on vCluster VDOM master on physical slave causes configuration mismatch and physical master overwrites.
539185	Modifying Login Challenge Page to include RADIUS attributes.
543503	RSSO user automatically gets added to a wrong user group.
546600	Cannot set certificate under `config certificate local`.
548460	`set device-identification disable` is reverted to default after VDOM restore.
549662	RADIUS MSCHAPv2 authentication fails on Windows NPS with non-ASCII characters in password.
550512	RSSO - wireless roaming causing undesirable removal of RSSO sessions.
554642	LDAP - search-type recursive does not retrieve nested membership through user's primary group.
554646	FSSO fabric connector needs to be renamed and needs to show connection status again.

VM

Bug ID	Description
537788	TCP re-transmission due to VMXNET3 RX ring buffer exhaustion.

Bug ID	Description
540641	FortiGate-VM deployed in OpenStack without bootstrapping doesn't have empty password.
542794	`Session size overflow` on VMX causing timeout and error on NSX vMotion task.
545533	FGT VMX: Default MTU of 65521 results in packet drops.
548366	Azure SDN fabric connector is showing status down.
548453	Ondemand platforms show error with FortiCare/FortinetOne login.
548531	FGT-AWS HA failover and SDN using IAM role do not work due to AWS IAM role token length being +increased.
550977	AliCloud: Native FortiGate HA A-P failover does not complete in Shanghai and Hangzhou.
559051	Azure `waagent` process consumes high memory.

VoIP

Bug ID	Description
544877	H323/H245 helper abnormal in `openLogicalChannel`.

Web Filter

Bug ID	Description
435951	Traffic keeps going through the `DENY` NGFW policy configured with URL category.
544342	When `encryption` is set to yes, `file-type` incorrectly shows all file types when only `zip` files are supported.
547772	Web filter FGD category is not detected by sniffer policy for HTTPS traffic.

WiFi Controller

Bug ID	Description
491390	FWF-60E crashes intermittently with no console access at the time.
509442	Suggest to input at least 12 characters when configuring pre-shared key for WPA/WPA2-Personal SSID.
516454	FortiGate doesn't send IPv6 router-advertisement towards one AP if the same SSID is being broadcast on two different APs.
526035	Standby FortiGate reporting rogue AP on wire.
537968	Region -N DFS support required for FAP-U422EV.
539916	TCP SYN+ACK is not forwarded under specific conditions.

Bug ID	Description
548101	CAPWAP tunnel does not get established on secondary IP address unless we enable CAPWAP access on primary IP address.
556451	Use firewall schedule (recurring, onetime, and group) to configure schedules for DARRP, disabling background rogue-AP scan, SSID, and FortiAP LED state.

Common Vulnerabilities and Exposures

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

Vulnerability
FortiOS 6.2.1 is no longer vulnerable to the issue described in the following link - https://fortiguard.com/psirt/FG-IR-19-144.

Bug ID	CVE references
503568	FortiOS 6.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2018-13367
532730	FortiOS 6.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2019-6693
539962	FortiOS 6.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2019-5591
548154	FortiOS 6.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2019-3855 • CVE-2019-3856 • CVE-2019-3857 • CVE-2019-3858 • CVE-2019-3859 • CVE-2019-3860 • CVE-2019-3861 • CVE-2019-3862 • CVE-2019-3863
555805	FortiOS 6.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2019-5593

Known Issues

The following issues have been identified in version 6.2.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Firewall

Bug ID	Description
541348	Shaper in shaping policy is not applied when URL category is configured.

FortiView

Bug ID	Description
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
526956	FortiView widgets get deleted upon upgrading to B222.
544017	FortiView > VPN 1 hour historical shows entries from 8 hours ago when logged in from FortiCloud.
555524	`ngfw-policy` cannot be traced in FortiView.
567049	*FortiView* > *Web Sites* view issue when VDOM works with NGFW policy mode.

GUI

Bug ID	Description
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
451776	Admin GUI has limit of 10 characters for OTP.

HA

Bug ID	Description
479987	FG MGMT1 does not authenticate Admin RADIUS users through primary unit (secondary unit works).

Intrusion Prevention

Bug ID	Description
445113	IPS engine 3.428 on FortiGate sometimes cannot detect Psiphon packets that iscan can detect.

IPsec VPN

Bug ID	Description
469798	The interface shaping with egress shaping profile doesn't work for offloaded traffic.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create web filter logs.

Proxy

Bug ID	Description
550056	When exempt SNI in SSL profile but SNI does not match CN, FortiGate closes the session and does not do deep inspection.
560893	When strict SNI check is enabled, FortiGate with certificate inspection cannot block session if SNI does not match CN.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the *Device* field.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.
476838	Check domain log-on as SSL VPN host checks condition.
495522	RDP session freezes when using SSL VPN tunnel mode.
564645	NGFW policy mode SSL VPN web portal traffic doesn't check security policy.
567073	SSL VPN web portal should remove Citrix and port forward connections option from GUI.

Switch Controller

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.

Bug ID	Description
357360	DHCP snooping may not work on IPv6.
462552	Add an extra dialog in the interface page to clean up config when changing a FortiLink interface back to a regular port.

System

Bug ID	Description
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
364280	User cannot use `ssh-dss` algorithm to login to FortiGate via SSH.
385860	FG-3815D does not support 1GE SFP transceivers.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
472843	When FortiManager is set for `DM = set verify-install-disable`, FortiGate does not always save script changes.
474132	FG-51E hang under stress test since build 0050.
494042	If we create VLAN in VDOM A, then we cannot create ZONE name with the same VLAN name in VDOM B.
563410	TP VDOM interfaces removed after upgraded image from build 1672 (v5.6.8) to build 0915 (v6.2.1).

Upgrade

Bug ID	Description
470575	After upgrading from 5.6.3, `g-sniffer-profile` and `sniffer-profile` exist for IPS and web filter.
473075	When upgrading, multicast policies are lost when there is a zone member as interface.
481408	When upgrading from 5.6.3 to 6.0.0, the IPv6 policy is lost if there is SD-WAN member as interface.
494217	Peer user SSL VPN personal bookmarks do not show when upgrade to 6.0.1. **Workaround**: Use CLI to rename the user bookmark to the new name.
539112	Devices configured under `security-exempt-list` become void after upgrade.

Web Filter

Bug ID	Description
538593	B0821: FGD service on https/8888 does not work well under specific wanopt topology.
545334	Web filter file filtering does not support FTP traffic inspection but user can still configure FTP protocol in GUI and CLI.

WiFi Controller

Bug ID	Description
560828	When the `dtls-policy=ipsec-vpn` is set, the FAP cannot be managed by FortiGate when VDOM type is policy based.

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.