FortiOS - Release Notes

Version 6.4.2

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

August 13, 2020
FortiOS 6.4.2 Release Notes
01-642-641039-20200813

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-07-30	Initial release.
2020-07-31	Updated *Changes in default behavior*, *New features or enhancements*, *Known issues*, and *Resolved issues*.
2020-08-04	Updated *Known issues*, *Resolved issues*, *New features or enhancements,* and *New FortiGuard anycast services*.
2020-08-05	Updated *Fortinet Security Fabric upgrade*.
2020-08-10	Updated *Changes in default behavior*, *New features or enhancements*, *New FortiGuard anycast services*, *Known issues*, and *Resolved issues*.
2020-08-11	Updated *New FortiGuard anycast services* and *Changes in default behavior*. Removed 618718 from *Known issues*.
2020-08-12	Added 656869 to *Known issues*.
2020-08-13	Added FWF-40F, FWF-40F-3G4G, FWF-60F, and FWF-61F to *Special branch supported models*.

Introduction and supported models

This guide provides release information for FortiOS 6.4.2 build 1723.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.2 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-61E
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, 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-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 6.4.2. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1723.

FWF-40F	is released on build 5323.
FWF-40F-3G4G	is released on build 5323.
FWF-60F	is released on build 5323.
FWF-61F	is released on build 5323.

Special notices

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.

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.

System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	• Removed *System* > *Advanced* menu (moved most features to *System* > *Settings* page). • Moved configuration script upload feature to top menu > *Configuration* > *Scripts* page. • Removed GUI support for auto-script configuration (the feature is still supported in the CLI). • Converted all compliance tests to security rating tests.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.2 has resolved bug 570575 to fix a FortiGate failing to provide power to ports. The PoE hardware controller, however, may require an update that must be performed using the CLI. Upon successful execution of this command, the PoE hardware controller firmware is updated to the latest version 2.18:

```
diagnose poe upgrade-firmware
```

AWS-On-Demand image

Bug ID	Description
589605	Starting from FortiOS 6.4.0, the FGT-VM64-AWSONDEMAND image is no longer provided. Both AWS PAYG and AWS BYOL models will share the same FGT-VM64-AWS image.

New FortiGuard anycast services

FortiOS 6.4.2 adds FortiGuard anycast services for geography IP, FortiToken Mobile, and DDNS. These services will be available by the end of August 2020.

To use these services before the FortiGuard anycast servers come online, please disable the `fortiguard-anycast` setting:

```
config system fortiguard
    set fortiguard-anycast disable
end
```

To continue using web filer when FortiGuard anycast is disabled, the port must be changed from 443 to 8888 or 53:

```
config system fortiguard
    set fortiguard-anycast disable
    set port 8888
end
```

Additionally, for DNS filtering, configure the SDNS server IP:

```
config system fortiguard
    set sdns-server-ip 208.91.112.220
end
```

Changes in CLI

Bug ID	Description
614892	Remove `spectrum-analysis` in `wtp-profile` and `override-analysis` in `wtp`.

621751	In a FortiSwitch LACP trunk, ports of the same negotiated speed are grouped into an aggregator. The `aggregator-mode` setting allows users to select the aggregator based on bandwidth or number of links.
	`config switch-controller managed-switch`
	`edit <serial_number>`
	`config ports`
	`edit <port>`
	`set mode lacp-passive`
	`set aggregator-mode {bandwidth | count}`
	`next`
	`end`
	`next`
	`end`

639237	EMS server can now generate dynamic address with MAC address in addition to IP address. The switch controller's NAC policy can reference MAC-based dynamic firewall address from EMS as a match condition.
	`config firewall address`
	`edit <name>`
	`set type dynamic`
	`set sub-type ems-tag`
	`set obj-type [ip | mac]`
	`next`
	`end`
	`config user nac-policy`
	`edit <ID>`
	`set category ems-tag`
	`set ems-tag <address>`
	`next`
	`end`

643514	The `hold-time` option allows users to set a hold time in hours or days to hold their signatures after a FortiGuard IPS signature update. During the hold period, the signature's action becomes monitor.
	`config system ips`
	`set signature-hold-time <##d##h>`
	`set override-signature-hold-by-id <enable|disable>`
	`end`

Bug ID	Description

643831	Enable users to filter IPS signatures based on CVE IDs (CVE-YYYY-NNNN), or by a CVE wildcard (CVE-YYYY).
	`config ips sensor`
	`edit "cve"`
	`config entries`
	`edit 1`
	`set cve <CVE ID or Wildcard>`
	`next`
	`end`
	`next`
	`end`

Changes in GUI behavior

Bug ID	Description
516031	The following behaviors regarding security profiles have changed: • Remove the *Feature Visibility* > *Multiple Security Profiles* option. • All security profiles will allow multiple profiles by default. • All security profile pages will be a list of profiles.
634719	Add the option to switch between optimal and comprehensive dashboard setups. This option is available in the login prompt when upgrading from an old FortiOS build or logging in as a new user. It can also be accessed any time after that from the *Reset All Dashboards* option available in the left navigation bar. *Optimal* offers a set of default dashboards and a pared down selection of *FortiView* pages. *Comprehensive* consists of a set of dashboards and all the *Monitor* and *FortiView* pages that were present in previous FortiOS versions.
643505	In the *Hub-and-Spoke* VPN wizard, add the ability to select multiple local interfaces, a step to review changes, and real-time updates when the tunnels are being created. Within the VPN dialog, add the *Hub-and-Spoke* topology section to display easy keys for each spoke and the ability to add additional spokes.

Changes in default behavior

Bug ID	Description

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

Changes in table size

Bug ID	Description
609785	Update number of supported FortiSwitch models per FortiGate platform.
626765	FG-60F/61F and FWF-60F/61F total WTP size is increased to 64.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
480717	Add `config system dedicated-mgmt` to all FortiGate models with mgmt, mgmt1, and mgmt2 ports.
556054	With the newly-added compression methods used in the CIFS messages, FortiGates can now scan these compressed messages in proxy mode.

562031	Support security policy `srcaddr-negate` and `dstaddr-negate` options, which can be configured under `firewall security policy`.
	`config firewall security-policy`
	`edit <policyid>`
	`...`
	`set srcaddr-negate[enable|disable]`
	`set dstaddr-negate [enable|disable]`
	`...`
	`next`
	`end`

573076	FortiGate generates a UUID for every managed FortiAP (WTP entry). A new BLE profile, `fortiap-discovery`, can facilitate iBeacon UUID deployment over FortiAP devices.
589621	New Azure on-demand and upgraded instances can retrieve a FortiGate serial number and license from FortiCare servers. Using the serial number, users can register the device to their account and start using FortiToken and FortiGate Cloud services.
596002	Add two new tables to the FortiOS enterprise MIB: FgSwDeviceEntry for details about connected FortiSwitches and FgSwPortEntry for port related information.
596870	Add kernel support for the IEEE 802.1ad (QinQ) standard. Previously, the 802.1Q standard allowed a single VLAN header to be inserted into an Ethernet frame. This new feature allows one more VLAN tag to be inserted into a single frame.
597301	Display information about autoscale members in the GUI and CLI, such as their serial number, IP address, instance ID, and transit gateway (AWS only).
600037	BSS coloring support on FAP-U431F/U433F (802.11ax AP).
608557	Support proxy server for push service.
610596	Users can define IPv6 MAC addresses and apply them in a firewall policy, virtual wire pair policy, and other policy types.
610990	Add IPv6 only and IPv4v6 dual stack support for GTPv1 and GTPv2 on FortiOS Carrier.

Bug ID	Description
614924	Users can configure automation with the *Quarantine via FortiNAC* action when setting triggers for *Compromised Host* or *Incoming Webhook*. When the automation is triggered, the client PC will be quarantined with its MAC address disabled in the configured FortiNAC.
617640	Add new filter keys `servicetag` and `region` in Azure SDN connector to filter out IP ranges of service tags. This can be applied to dynamic firewall addresses.
620994	For FortiAP models with three radios, spectrum analysis can be performed on the thrid radio on all channels from the 2.4 GHz and 5 GHz bands. On FortiAPs with two radios operating in AP mode, spectrum analysis can be performed on operating channels.
621714	For the purpose of communicating timing precision between two ends, transparent clock can be enabled to measure the overall path delay. This feature allows the FortiGate to configure this setting for supported FortiSwitch models.
621742	Add support to configure the FortiSwitch to send multiple RADIUS attribute values within a single RADIUS access request.
621746	Support explicit congestion notification (ECN) configuration for managed FortiSwitch.
621757	Add support to configure switch ports to enable inter-operability with rapid PVST+ on managed FortiSwitches.
622291	Health metrics calculations are standardized in the backend, and consistent colors are used to represent good, fair, and poor metrics. In addition, the health data is now available through a REST API.

623821	For WiFi clients associated with a bridge SSID on a FortiAP that is connected to an Ethernet interface of a FortiGate, the *DHCP Monitor* widget can indicate the AP bridge and the SSID name in the *Interface* column of those clients' IP leases.
	In the CLI, `dhcp-option43-insertion` is added under VAP configuration to support this feature.
	`config wireless-controller vap`
	`edit VAP01`
	`set dhcp-option43-insertion {enable | disable}`
	`next`
	`end`
	By default, `dhcp-option43-insertion` is set to enable.

629530	Support running BYOL FortiGate VMs on IBM Cloud platform.
630238	Allow configuration of up to 16 FGSP standalone peers in `system standalone-cluster`.
630881	Various new scenarios are added in Security Rating to test the FortiSwitch network and make recommendations to optimize the setup.
631818	Add new OIDs to support SNMP queries for IPv4 and IPv6 IPsec tunnels, and SNMP queries for license details.
635717	Monitoring FortiAP antenna (per Rx chain) status and logging wireless events upon antenna defect detection.

Bug ID	Description
635795	The ARRP profile improves upon DARRP by enabling more factors to be considered for optimizing channel selection among FortiAPs.
637946	Replace previous slide-out terminal with a full page masking terminal. Allow admins to open multiple CLI consoles that can be minimized.
638975	SD-WAN and policy route now allow users to choose the device MAC address object as source. In addition, the FABRIC_DEVICE object can also be used in SD-WAN and policy route.
639590	In NGFW mode application control logs will be generated when an application, application category, or application group is selected on a security policy and log traffic is set to UTM or all. In addition, when one signature is accepted under the security policy, all child signatures are assessed and logged correspondingly.
640320	Add FortiAP platform support for FAP-231F.
640563	The default command to restrict FortiLink interfaces to one interface has been removed. The GUI will now display multiple FortiLink interfaces if more than one interface has FortiLink enabled from the CLI.
641152	New bandwidth-limited VM licenses allow VM deployments with limited bandwidth usage per interface. Dedicated management interfaces are exempt from calculation.
641990	The `diagnose wad session list` command is available in models without WANopt support.
642898	The following options are configurable in the flow-based web filter security profile in NGFW policy mode, and they can be applied to a security policy: • *Block invalid URLs* • *Static URL Filter* • *Block malicious URLs discovered by FortiSandbox* • *Content Filter*
643616	Support FortiAP to query FortiGuard IoT service through FortiGate to determine device details.
643912	Sometimes it is necessary to map a VIP to an FQDN address. This setting can now be configured from the GUI.
644049	Enhancements to multiple pre-shared key per SSID include the ability to batch generate or import MPSK keys, export keys to CSV, dynamically assign VLANs based on the MPSK used, and to apply an MPSK schedule in the GUI.
645140	Tunnel ID is added to traffic logs and GTP logs for GTP related traffic in order to correlate the sessions.
648568	In additional to servers added in 6.4.0, FortiGuard servers for GeoIP, DDNS, and FortiToken Mobile registration now support third-party CA signed certificates with OCSP stapling.
648604	For user location information (ULI) in GTP, it may contain more than one identity of different type. This log enhancement displays all identity information in GTP logs.
651206	The GUI in the downstream FortiGate allows users to log in to the Fabric root device to authorize a pending join request.

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.

In 6.4.0, device detection related GUI functionality has been relocated:

1. The device section has moved from *User & Authentication* (formerly *User & Device*) to a widget in *Dashboard*.
2. The email collection monitor page has moved from *Monitor* to a widget in *Dashboard*.

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

- FortiAnalyzer 6.4.2
- FortiManager 6.4.2
- FortiClient EMS 6.4.1 build 1487 or later
- FortiClient 6.4.1 build 1511 or later
- FortiAP 6.0.6 build 0075 or later
- FortiSwitch 6.0.6 build 0076 or later

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC
14. FortiNAC

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.2. When Security Fabric is enabled in FortiOS 6.4.2, all FortiGate devices must be running FortiOS 6.4.2.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.2 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 6.4.2 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 6.4.2 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 6.4.2 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 6.4.2, 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 6.4.2.

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 Hypervisor 8.1 Express Edition

- `.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 Server 2019 and Windows Server 2012R2 with Hyper-V role

- `.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. 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

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

- Optimal: Default dashboard settings in 6.4.1
- Comprehensive: Default Monitor and FortiView settings before 6.4.1

WanOpt configuration changes in 6.4.0

Port configuration is now done in the profile protocol options. HTTPS configurations need to have certificate inspection configured in the firewall policy.

In FortiOS 6.4.0, `set ssl-ssh-profile certificate-inspection` must be added in the firewall policy:

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.2.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

Product integration and support

The following table lists FortiOS 6.4.2 product integration and support information:

Web Browsers	• Microsoft Edge 83 • Mozilla Firefox version 76 • Google Chrome version 83 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 20. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 6.4.2 must work with FortiManager 6.4.1 or later. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 20. 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 20 and Fortinet Security Fabric upgrade on page 20. 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
FortiClient EMS	• 6.4.0
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later

FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later
FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0291 and later (needed for FSSO agent support OU in group filters) • Windows Server 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	• 3.2.1
AV Engine	• 6.00149
IPS Engine	• 6.00032
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
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 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 78 Google Chrome version 84
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 78 Google Chrome version 84
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
OS X Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 78 Google Chrome version 84
iOS	Apple Safari Mozilla Firefox

Operating System	Web Browser
	Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 6.4.2. For inquires about a particular bug, please contact Customer Service & Support.

Anti Spam

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

Anti Virus

Bug ID	Description
560044	Secondary device blades occasionally report critical log event `Scanunit initiated a virus engine/definitions update`. Affected models: FG-5K, 6K, and 7K series.
607432	500 internal error for some PDFs with AV applied.
615805	Device goes into conserve mode due to large files.
635535	Scanunit crashes with signal 14 at `sys_fortiuser_cmd > get_iprope_mem_conserve`.

Application Control

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

Data Leak Prevention

Bug ID	Description
629713	DLP filters not matching in order if a `file-type` filter is configured.

DNS Filter

Bug ID	Description
511729	Domain filter entries whose action is set to allow should not be logged.
613024	DNS logs do not contain response code.

Endpoint Control

Bug ID	Description
640142	FortiOS 6.4 cannot verify EMS cloud certificate.

Explicit Proxy

Bug ID	Description
634515	HTTP 1.1 host header is lost in FortiGuard web proxy requests.

File Filter

Bug ID	Description
627795	In flow mode, file filter log can show the file type, but when in proxy inspection mode, it only shows unknown file type.

Firewall

Bug ID	Description
590039	Samsung OEM internet browser cannot connect to FortiGate VS/VIP.
595949	Any changes to the security policy table causes the hit count to reset.
596633	In NGFW mode, IPS engine drops RPC data channel when IPS profile is applied to a security policy.

Bug ID	Description
606962	Timeout value is not reflected correctly to a new session when changing timeout value for `system session-ttl` on FortiGate-HV.
628841	Internet service entry not detected due to some IP ranges being duplicated.
633856	Sessions are marked dirty when IPsec dialup client connects/disconnects and policy routes are used.
635007	Updates causing conserve mode.
643841	DCE RPC helper cannot parse fragmented EPM packet.
644638	Policy with Tor-Exit.Node as source is not blocking traffic coming from Tor.
644865	Query string parameters omitted (HTTP redirect, SSL offloading).
645075	Real server byte counter resetting.

FortiView

Bug ID	Description
573138	When the data source is FortiGate Cloud, there is no paging to load sessions; only entries 1-499 are rendered.
615524	*FortiView > All Sessions* should be supported as a standalone dashboard widget in navigation bar.
639109	*Top Countries/Regions by Bytes* widget keeps trying to load.
640759	Unable to filter FortiView sessions in FortiOS 6.4.x.

GUI

Bug ID	Description
513694	User cannot log in to GUI when password change is required and has pre-login or post-login banner enabled or FIPS mode.
516031	The following behaviors regarding security profiles have changed: • Remove the *Feature Visibility > Multiple Security Profiles* option. • All security profiles will allow multiple profiles by default. • All security profile pages will be a list of profiles.
528145	BGP configuration gets applied on the wrong VDOM if user switches VDOM selection in between operations (slow GUI).
541042	Log viewer *Forward Traffic* cannot support double negate filter (client-side issue).

Bug ID	Description
547697	Inconsistency/confusion regarding *Hostname* field in FortiOS web filter log.
567936	Saved SMS phone number is missing + for country code.
577991	Dotted line shown between FortiGate and second tier switch in *Managed FortiSwitch* topology.
592073	LED indications for FortiSwitch ports do not auto-reflect the changes made on PoE.
594534	GUI shows *Invalid LDAP server* error while LDAP query successfully finished.
594702	When sorting the interface list by the *Name* column, the ports are not always in the correct order (port10 appears before port2).
594991	New service group for explicit proxy could not be saved from GUI.
601568	Interface status is not displayed on faceplate when viewed from *System* > *HA* page.
601879	Get *The web page cannot be found* error after factory reset.
604682	GUI takes two minutes to load *VPN* > *IPsec Tunnels* for 1483 tunnels.
605030	*Send Logs to FortiCloud* and *Cloud Logging* options not available in GUI for FG-900D.
605496	Configured overlapped subnet on GUI still shows error message after enabling subnet overlap.
606967	One-time schedules are not displayed correctly in Safari browser.
607296	Firewall address keeps loading addresses with read-write permission.
607549	GUI CMDB API to support case sensitive/insensitive filtering.
612236	RADIUS test in GUI does not use configured authentication method and test fails.
615267	In Firefox, SAML SSO admin cannot create additional SSO admins or normal admins via the GUI.
616878	DHCP relay IP address not showing on *Network* > *Interfaces* page for VLAN interface.
618379	Option for TLS in Fortinet FSSO connector does not change port to CA TLS port 8001.
618617	CLI parser error: `shaper-profile` default class with 0% bandwidth guarantee only possible in GUI.
620854	GUI should not add speed to virtual switch member port (FG-101F).
621902	Default gateway address of DHCP server setting does not follow the interface address when *Same as Interface IP* is selected.
623109	IPS *Filter Details* column is empty when *All* is used.
623939	Interface bandwidth widgets for WAN, PPPoE and VDOM link interfaces are not loading.
624050	FortiGuard page does not open with custom read-write permission in the account profile (403 forbidden error).
624551	On POE devices, several sections of the GUI take over 15 seconds to fully load.
624662	CLI panel allows read-only managed device to be configured by read-only admin.
628373	Software switch members and their VLANs are not visible in the GUI interfaces list.

Bug ID	Description
629139	*Security Rating* reports should not run as a dependent of *Topology* reports on downstream FortiGates.
630638	Add a warning when *Capture Packets* is enabled in policy dialog.
631734	GUI not displaying PoE total power budget on FOS 6.2.3.
633937	GUI is not displaying DHCP configuration if the interface name includes the \ character.
634677	User group not visible in GUI when editing the user with a single right-click.
635538	In FortiGate SAML authentication with Azure AD, SP configuration is grayed-out in the GUI.
638034	Ctrl + V does not paste command in GUI CLI console and Ctrl + C does not copy selected output in CLI console.
638277	Firewall address group object (including interface subnet) is invisible in *Accessible Networks*.
638615	SSO admin cannot open CLI console.
638911	IPS and application control actions cannot be modified to *Quarantine*.
639129	IPsec aggregate is not shown in *Dashboard* > *Network* > *IPsec* widget.
639163	GUI does not show user group information on firewall user widget.
639288	No historical sessions can be displayed when FortiView widget opens from *Show in FortiView.*
639542	The *Edit* pane for *PAC File Content* on the *Explicit Proxy* page cannot be opened.
642028	On some platforms (FG-60E-61E/81E), the CLI console in the GUI may not function immediately after bootup.
642402	LCP-1250RJ3SR-K transceiver shows a warning in the GUI even though it is certified.
644999	Fortinet-sold active direct attached cable (SP-CABLE-ADASFP+) is showing as not certified by Fortinet.

HA

Bug ID	Description
595340	hasync process consuming 80-95% CPU.
609631	Simultaneous reboot of both nodes in HA when `gtp-enhance-mode` enabled or disabled.
627610	When HA primary device is down, a time synchronization with NTP servers will be disabled after failback.
627851	After the HA peer node has been replaced, need a way to reset the HA health status back to OK.
630070	HA is failing over with crashes.
631342	FG-100D HA active-passive mode not syncing.

Bug ID	Description
634604	SCTP sessions are not fully synchronized between primary and secondary devices in version 5.6.11 on FG-3240C.
637843	HA secondary device is reporting multiple events (DDNS update failed).
638287	`private-data-encryption` causes cluster to be periodically out of sync due to customer certificates.
639307	Both primary and secondary consoles keep printing `get_ha_sync_obj_sig_4dir: stat /etc/cert/ca/5c44d531.0 error 2`.
640428	SSL VPN related auth login user event logs do not require HA to be in sync.
643958	Inconsistent data from FFDB caused several confsyncd crashes.
645293	`traceroute` not working in asymmetric FGSP environment.
645387	HA `pingsvr` is in up state in spite of `lnkmtd` showing it as being in die state.
648073	HA cluster uses physical port MAC address at the time of HA failover.

Intrusion Prevention

Bug ID	Description
582936	IPS traffic log and PCAP archive do not match.
595062	SSL offloading randomly does not work when UTM (AV/IPS) is enabled in firewall policy.
617588	Unable to open TCP application via IPsec tunnel when `np-accel-mode` is enabled.
631381	RDP NLA authentication blocked by FortiGate when enabling IPS profile in the security group (central NAT).
638235	Some IPS logs do not include direction field.

IPsec VPN

Bug ID	Description
516029	Remove the IPsec global lock.
610203	Packet loss on IPsec tunnel.
622959	FortiGate does not send framed IPv6 address in RADIUS accounting records.
631804	OCVPN errors showing in logs when OCVPN is disabled.
631968	IKE daemon signal 6 crash when `phase1 add-gw-route` is enabled.

Bug ID	Description
634883	IKE crashes at `ike_hasync__xauth`.
635325	Static route for site-to site VPN remains active even when the tunnel is down.
645196	IPsec routes are restored to the routing table automatically for tunnels that are not connected.

Log & Report

Bug ID	Description
589782	IPS sensor `log-attack-context` output truncated.
605405	IPS logs are recorded twice with TCP offloading on virtual server.
607449	Log searches being conducted in a FortiGate for logs stored on a FortiAnalyzer are only sent as case-sensitive.
630769	miglogd crashes when the FortiGate does a weekly log purge.
634947	rlogd signal 11 crashes.
635013	FortiOS gives wrong time stamp when querying FortiGate Cloud log view.
637117	Incomplete log field returned from CEF formatted syslog message.
639807	PBA logs show only 0 or 1 duration in logs; cannot answer data requests from law enforcement.
641450	miglogd processes bound to busy CPUs even though there are other completely idle CPUs available.

Proxy

Bug ID	Description
586281	WAD memory corruption.
603195	Multiple WAD crashes with signal 11.
623108	FTP-TP reaches high memory usage and triggers conserve mode.
624245	WAD crashes when all of these conditions are met: policy is doing deep inspection, SNI in client hello is in the exempt list, server certificate CNAME is not in the exempt list.
631542	WAD signal 11 crash logs SSL/TLS errors and disconnects with the OCSP stapling.
633175	WAD crash observed, `wad_http_pattern_match_response + 0x0045`, on FG-80E-POE during regression testing.
636508	FortiGate blocks traffic in transparent proxy policy, even if the traffic matches the proxy address.

Bug ID	Description
637389	The WAD process is crashing multiple times.
640427	Web proxy WAD crash under WAN Opt auto-active mode.
643725	The IMAP proxy crashes with signal 7 (SIGBUS).
645943	Memory usage spike (all WAD workers) without bandwidth spike.

Routing

Bug ID	Description
624621	Log traffic to remote servers does not follow SD-WAN rules.
627951	NTP and FSSO not following SD-WAN rules.
628896	DHCP relay to follow SD-WAN rules.
633463	DRother firewall in OSPFv3 generates `neighbor state is less than Exchange` log for the LSA update from a DCother neighbor.
633600	BGP hold time and keepalive timers are not updated on spokes after changing on the hub side.
635716	FortiGuard web filter traffic also needs to follow SD-WAN service.
639834	Inconsistency in source IP-based ECMP for IPv6.
641022	Multiple duplicate routes in kernel causing conserve mode.
641928	Wrong behavior with SD-WAN routing on FG-60F.
646418	SD-WAN information available in session list is confusing.

Security Fabric

Bug ID	Description
619696	Automation stitch traffic is sent via `mgmt` with `ha-direct` to AWS Lambda after upgrading from 6.0.9 to 6.2.3
622032	SSH as automation action is not working as expected.
626691	FG-60F unable to join Security Fabric, unknown CA.
631607	CSF root FortiGate cannot listen to loopback interface.
637464	FortiMail appears as *Unknown fabric device* when `multi-vdom` is enabled.

Bug ID	Description
638512	User sees a *Failed to send request* error when generating access token for FortiMail under multi-VDOM FortiGate.
641006	Automation stitch causes HA sync failure.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page titled {{::data.portal.heading}} after authentication.
573853	TX packet drops on SSL root interface.
604772	SSL VPN tunnel is unexpectedly down sometimes when certificate bundle is updated.
608464	Get 305 error when browsing website through SSL VPN web mode bookmark and sslvpnd crashes.
611498	SMB/CIFS traffic via SSL VPN web mode not using correct SNAT IP (IP pool).
613612	Important GUI pages in 6.4.0 are not rendered well by SSL VPN portal.
620508	CLI command `get vpn ssl monitor` displays users from other VDOM.
622110	SSL VPN disconnected when importing or renaming CA certificates.
623076	Add memory protection for web mode SSL VPN child process (guacd).
623217	Website pop-up error using SSL VPN web mode.
623379	Memory corrupt in some DNS callback cases causes SSL VPN crash.
624283	Customer has to manually add domain in SMB share login through SSL VPN portal.
624899	Log entry for tunnel stats shows wrong tunnel ID when using RDP bookmark.
626228	Bookmark does not load though SSL VPN web mode.
626237	SAP portal link is not working in SSL VPN web mode.
627150	SSL VPN web mode unable to load custom web application JavaScript parts.
627456	Traffic cannot pass when SAML user logs in to SSL VPN portal with group match.
628059	SSL VPN web mode gets redirected out of SSL VPN proxy.
628597	Unable to load the SSL VPN bookmark internal website https://fi***.
628801	Internal web application is not opened after the login.
628821	Internal aixws7test2 portal is not loading in SSL VPN web mode.
629190	After SSL VPN proxy, some JS files of hapi website could not work.
629373	SAML login button is lost on SSL VPN portal.

Bug ID	Description
630432	Slides in website https://re***.nz are displayed in SSL VPN web mode.
631050	ERR_EMPTY_RESPONSE while accessing internal portal's webpages in SSL VPN web mode.
631130	Internal site http://va***.com not completely loading through SSL VPN web mode bookmark.
631402	Website (https://uj***) is not accessible in SSL VPN web mode.
631510	Some internal servers do not provide any content type or content length in response header; sslvpnd treats it as HTML file to handle and has problem to finish it.
631809	Configuring thousands of `mac-addr-check-rule` in portal makes the CPU spike significantly if several hundreds of users are connecting to the FortiGate, thus causing SSL VPN packet drops.
633047	Cannot load local 1C application through web mode.
633114	Cannot access internal website pl***.fr using SSL VPN web mode.
633812	For guacd daemon generated for RDP session, it would sometimes be in an unknown state with 100% CPU and could not be released.
634210	SSL VPN daemon crash due to `limit-user-login`.
634991	Internal server error 500 while accessing contolavdip portal in SSL VPN web mode.
635307	Map could not be displayed correctly in SSL VPN web mode.
635341	SSL VPN not assigning IP from local IP pool when framed IP address is received with value 0xFFFFFFFE.
635608	Map could not be displayed correctly in SSL VPN web mode.
635896	The sa***.org website is not shown properly in SSL VPN web mode.
635899	SharePoint portal URL links for Office documents are not redirected over SSL VPN web mode in Firefox.
635907	AM*** website is not shown properly using SSL VPN web mode.
636332	With SSL VPN proxy JIRA web application, get one wrong URL without proxy path.
636984	Website (pr***.com) not loading properly in SSL VPN web mode.
637018	After the upgrade to 6.2.4/6.4.0 SSL VPN portal mapping/remote authentication is matching user into the incorrect group.
637164	The customer's website (https://vpn.***.org) is not shown properly using SSL VPN web mode.
638733	Internal website hosted in bookmark https://in***.cat is not loading completely in SSL VPN web mode.
639431	Three of the internal applications/portal bookmarks do not load/partially work with SSL VPN web mode.
639768	Log in page loading with delays in web mode.
639789	Apache Guacamole page is redirected to direct link in SSL VPN web mode.
640167	The Run*** website is not displayed properly using SSL VPN web mode.

Bug ID	Description
642225	The IC*** internal website is not displayed properly using SSL VPN web mode.
643598	Application is not working using SSL VPN web mode.
643749	SSL VPN crashes when accessing a realm with an incorrect user, or when the correct user enters the wrong password.
644506	Cannot authenticate to SSL VPN using 2FA if remote LDAP user and user within RADIUS group has same user name and password.
644607	Sco*** internal portal webpage is not loading after logging in with web mode.
645276	After SSL VPN web mode proxy, some JS files of sthlm04 SCA*** website have problems.
646429	Update Telnet idle timeout setting and fix issue of Telnet not working.
647296	SSL VPN web mode problem with https://de***.com.
648369	Some JS files of ji***.v** could not run in SSL VPN web mode.
649197	Unable to use editor in Atlassian internal Confluence portal over SSL VPN web mode.
649466	SSL VPN authentication fails when `all-usergroup` is enabled in RADIUS server.

Switch Controller

Bug ID	Description
633842	FortiLink down with LACP mode set to active.
646178	It is possible to view information of shared FortiSwitch ports in a tenant VDOM from the GUI, but there should not be recommended configuration changes in the GUI. Please use CLI for configuration changes.

System

Bug ID	Description
506485	FortiOS `get system interface cross-check` command improvement.
552788	DSL route not removed when interface is down.
567019	CP9 VPN queue tasklet unable to handle kernel NULL pointer dereference at 0000000000000120 and device reboots.
572847	The wan1, wan2, and dmz interfaces should not be configured as hardware switch members on the 60F series. The wan interface should not be configured as a hardware switch member on the 40F series.

Bug ID	Description
594264	NP-offloaded active TCP/UDP sessions established over IPsec VPN tunnels will timeout at session TTL expiry.
594871	Potential memory leak triggered by FTP command in WAD.
596209	Device has become unmanageable; receiving `errno=Resource temporarily unavailable` when trying to update objects.
598928	FortiGate restarts FGFM tunnel every two minutes when FortiManager is defined as FQDN.
605723	FG-600E stops sending out packets on its SPF and copper port on NP6.
611512	When a LAG is created between 10 GE SFP+ slots and 25 GE SFP28/10 GE SFP+ slots, only about 50% of the sessions can be created. Affected models: FG-110xE, FG-220xE, and FG-330xE.
612302	FortiOS is not sending out IPv6 router advertisements from the link-local addresses added on the fly.
613017	`ip6-extra-addr` does not perform router advertisement after reboot in HA.
615586	Incorrect IP/MAC address on ESXi hosts.
617134	Traffic not showing statistics for VLAN interfaces based on hardware switch.
617154	Fortinet_CA is missing in FG-3400E.
618158	DHCP client cannot get IP address when NTP server option in DHCP server settings is set to *Same as System NTP*.
618762	Fail to detect transceiver on all SFP28/QSFP ports. Affected platforms: FG-3300E and FG-3301E.
626371	Request to blocked signature with SSL mirrored traffic capture causes FG-500E to reboot.
626785	FG-101F should support the same WTP size (128) as the FG-100F.
627054	HTTPSD signal 6 crash in cases of long application lists that are greater or equal to the maximum size of 16.
627409	Cannot create hardware switch on FG-100F.
627629	DHCP client sent invalid DHCP-REQUEST format during INIT state.
628642	Issue when packets from same session are forwarded to each LACP member when NPx offload is enabled.
630658	Auto-script output file size over 400 MB when configured output size is default 10 MB.
632353	Virtual WAN link stops responding after 45 members.
632407	Cannot delete VDOM due to ssl.vdom1 interface after changing mode from split-task VDOM to multi VDOM.
632635	Frame size option in sniffer does not work.
633102	DHCPv6 client's DUID generated on two different FortiGates match.
633298	10G ports x1/x2 cannot be set as interfaces in firewall `acl`/`acl6` policies.

Bug ID	Description
634415	Speed of 100G in `get system interface cross-check` shown incorrectly as `34464` for Fortinet-authorized FINISAR CORP FTLC9551REPM.
634494	`accprofile` permission for `config system link-monitor` is not correct.
634495	`accprofile` permission for `execute ping` is not correct.
636069	Unable to handle kernel NULL pointer dereference at 000000000000008f.
637420	`execute shutdown` reboots instead of shutting down on SoC4 platforms.
638041	SFP28 port group (ha1, ha2, port1 and port2) missing `1000full` speed option. Affected platforms: FG-220xE, FG-330xE, FG-340xE, and FG-360xE.
638738	In VDOM, `config log syslogd xxx` is not shown in `show full-configuration`.
639623	Possible conflicts between software switch VLAN setting and its member interface VLAN setting.
641419	FG-40F LAN interfaces are down after upgrading to 6.2.4 (build 5632).
643188	Interface `forward-error-correction` setting not honored after reboot.
645363	SNMP monitoring does not provide the SD-WAN member interface name.
647593	After reboot, `forward-error-correction` value is not maintained as it should be.
647718	VDOM with long name cannot be deleted.
647777	FortiGate not responding to DHCP relay requests from clients behind a DHCP relay.
649506	Sometimes FortiGate does not boot when restoring configuration using private data encryption.

Upgrade

Bug ID	Description
635589	Upon upgrading to FortiOS 6.2.4, DoS policies configured on interfaces may drop traffic that is passing through the DoS policy configuration. Note that this can occur if the DoS policy is configured in drop or monitor mode. **Workaround:** disable the DoS policy.

User & Authentication

Bug ID	Description
597319	In SSL VPN certificate authentication, add auth policies in base of LDAP group.
605838	Device identification scanner crashes on receipt of SSDP search.

Bug ID	Description
620941	Two-factor authentication using FortiClient SSL VPN and FortiToken Cloud is not working due to push notification delay.
625107	No response when using FTM-PUSH because unable to set source IP for FTM-PUSH.
627144	Remote admin LDAP user login has authentication failure when the same LDAP user has local two-factor authentication.
629487	Older FortiGate models do not have CA2 and will cause EMS server authentication to fail.
634580	Peer users are matching every group instead of only groups based on the LDAP group membership.
635385	In HA cluster, RADIUS accounting not working with `use-management-vdom enable`.
637577	Inconsistent fnbamd LDAP group match result.
638593	Certificate verification fails if any CA in a peer-provided certificate chain expires, but its cross-signed certificate is still valid in the system trust store.

VM

Bug ID	Description
587180	FG-VM64-KVM is unable to boot up properly when doing a hard reboot with the host.
603100	Autoscale not syncing certificate among the cluster members.
623376	Cross-zone HA breaks after upgrading to 6.4.0 because upgrade process does not add relevant items under `vdom-exception`.
624657	Azure changes FPGA for Accelerated Networking live and VM loses SR-IOV interfaces.
626705	By assigning port1 as the HA management port, the HA secondary unit node is now able to send system information to the Azure portal through waagent so that up-to-date information is displayed on the Azure dashboard. If port1 is not used as the HA management port, the Azure display and Azure Security Center alerts will not reflect the correct state of the node, which may result in unnecessary alarms.
629709	AWS VM stops processing traffic in some interfaces when running `diagnose debug application ike -1`.
634245	Dynamic address objects are not resolved to all addresses using Azure SDN connector.
634499	AWS FortiGate NIC gets swapped between port2 and port3 after FortiGate reboots.
641038	SSL VPN performance problem on OCI.
653567	Admin cannot log in to FortiGate VM GUI after license expired.

VoIP

Bug ID	Description
643548	SIP transfer calls fail when extensions are behind the same FortiGate (spoke).

Web Filter

Bug ID	Description
576862	Update `urlfilteridx` in traffic log to be `webfilter.urlfilter.entry.id`.
611501	Clarify meaning of `urlfilteridx=0` log field when proxy-based inspection is used.
621807	*Filtering Services Availability* status is down on the GUI when HTTP/80 is used for web filtering rating service.
625897	*Filtering Services Availability* status is down on the GUI when HTTP/80 is used for web filtering rating service.
629005	foauthd has signal 11 crashes when FortiGate does authentication for a web filter category.
630232	Certain regex static URL entries stopped working in 6.2.3.
636754	If the last line in a threat feed does not end with `\n`, it is not parsed and is not displayed in the GUI.
647227	Externally imported list (custom threat feed) is matching incorrectly in web filter remote category.

WiFi Controller

Bug ID	Description
605937	WiFi health monitor *Client Count* widget shows clients on the wrong band (on local standalone SSID).
625326	FortiAP not coming online on FG-PPPoE interface.
638537	*Applications*, *Destinations*, and *Policies* keep loading for *WiFi Clients* > *Diagnostics and Tools* drill-down.
641811	In FG-100F/101F with PPPoE interface, the FortiGate could not manage FortiAP.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
558685	FortiOS 6.4.2 is no longer vulnerable to the following CVE Reference: • CVE-2020-12812

Known issues

The following issues have been identified in version 6.4.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Data Leak Prevention

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

DNS Filter

Bug ID	Description
643521	DNS filter may encounter delays when connecting to Anycast servers over TLS/853. Workaround: Disable the anycast server or allow the rating error.

Explicit Proxy

Bug ID	Description
654211	When the category proxy address is applied in a proxy policy, if SOCKS traffic passes through the web proxy, when matching the SOCKS traffic with the proxy address, the WAD will crash with signal 11 at wad_url_choose_cate. Browsers may send SOCKS traffic in the background from time to time.

Firewall

Bug ID	Description
609027	SCTP secondary path not working in ECMP context; incorrect expectation session created from auxiliary session.
616220	ICMP reply packets dropped by the FortiGate.
653897	VIPs are removed from policy destination address after upgrading to 6.4.1.

FortiView

Bug ID	Description
645839	FortiView GUI not loading the *Sources* and *Destinations* pages (with *IPs* and *now* filters).

GUI

Bug ID	Description
446427	Failed to update VDOM license in GUI if the new license has lower VDOM count than the current license.
547123	The help message of `gui-dynamic-profile-display` is not correct.
561889	Firewall address object in GUI is not displaying *Invalid Subnet Mask* error when it should.
567996	GUI issues with physical topology on *Managed FortiSwitch* and *FortiSwitch Ports* pages.
606814	Security profile group does not switch from *certificate-inspection* to *no-inspection* in the GUI.
612066	*Entry not found* error shown when adding SSL VPN tunnel interface to *Multicast*.
651412	Print option in *Guest Management* page does not work; send options for SMS and email are OK.
654186	In *Device Inventory Monitor* dashboard, no device information shown in inventory chart when visualization set to table.
654256	*Interfaces* speed test fails and get *Failed Dependency* error when it has multiple VDOMs.
654626	It is impossible to change the *Action* setting using the *FortiGuard Category Based Filter* on a *DNS Filter Profile* page.
655568	GUI does not allow users to deselect *Administrative Access* options for VLAN interfaces.
655891	Web CLI console does not work if port 8080 is being used.

HA

Bug ID	Description
653642	FortiGate HA failover from FortiManager is not successful.
656099	After upgrading firmware to 6.4.2, missing heartbeat interface mgmt1 in the GUI, and CLI does not allow appending it with mgmt.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.

Log & Report

Bug ID	Description
643840	`vwlservice` should log the SD-WAN rule and not an internet service; impacts FortiAnalyzer SD-WAN monitor widgets and reports.

Proxy

Bug ID	Description
648831	WAD memory leak on FortiOS 6.2.4.

Routing

Bug ID	Description
641050	Need support for SSL VPN web mode traffic to follow SD-WAN rules/policy route.

Security Fabric

Bug ID	Description
652737	FortiGate does not send interface configuration to FortiIPAM.
654215	*FortiAnalyzer Cloud Solutions* links should redirect to the correct AWS/Azure/GCP URLs instead of the FortiGate IP address.

SSL VPN

Bug ID	Description
550819	guacd is consuming too much memory and CPU resources during operation.
649130	SSL VPN log entries display users from other VDOMs.

Switch Controller

Bug ID	Description
607753	CAPWAP is not updated to be a Fabric connection after upgrading from 6.4.0 Beta1 build 1519 to build 1538.
621785	`user.nac-policy[].switch-scope` may contain a data reference to `switch-controller.managed-switch`. When this reference is set by an admin, they need to remove this reference prior to deleting the `managed-switch`.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
555616	TCP packets sent out wrong interface and high CPU.
587824	Member of virtual WAN link lost after upgrade if management interface is `set dedicated-to management` before.
594577	Out-of order packets for an offloaded multicast stream.
627269	Wildcard FQDN not resolved on the secondary unit.
642005	FortiGate does not send `service-account-id` to FortiManager via fgfm tunnel when FortiCloud is activated directly on the FortiGate.
642327	FortiGate unable to boot with kernel panic by cmdbsvr when VLAN is configured on redundant interface with non-NPU port.
644380	FG-40F/60F kernel panic: `failure at mm/vmalloc.c:1341/__get_vm_area_node()!.`
644782	A large number of detected devices causes httpsd to consume resources and enter conserve mode.
647309	Kernel crash at `filter4` module and subsequent loop of `failure at mm/vmalloc.c:1341/__get_vm_area_node()!.`
651103	FG-101F crashed and rebooted when adding `vlan-protocol 8021ad` VLAN.

Upgrade

Bug ID	Description
618809	Boot up may fail when downgrading from FOS 6.4.0 to 6.2.3.
656869	FG-100F/101F may continuously boot upon upgrading from FortiOS 6.4.0. **Workaround**: back up the 6.4.0 configuration, perform a clean install via TFTP of FortiOS 6.4.2, and restore the 6.4.0 configuration.

User & Authentication

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW mode.
655422	A space after a comma within `CN` is incorrectly removed during the bind request causing authentication failure (LDAP).

VM

Bug ID	Description
617046	FG-VMX manager not showing all the nodes deployed.
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).
646161	FG-VM8 does not recognize all memory allocated in Hyper-V.
652416	AWS Fabric connector always uses root VDOM even though it is not a management VDOM.

Web Filter

Bug ID	Description
654160	Web filter profile count decreased after upgrading to 6.4.0 on FG-100F.

WiFi Controller

Bug ID	Description
647703	HTTPS server certificate is not presented when WiFi controller feature is disabled in *Feature Visibility*.
656804	Spectrum analysis disable/enable command removed in CLI from *wtp-profile* and causing a bottleneck for APs, such as FAP-222C/223C at 100% CPU.

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.