FortiOS - Release Notes

Version 6.4.13

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

June 8, 2023
FortiOS 6.4.13 Release Notes
01-6413-902132-20230608

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-06-08	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 6.4.13 build 2092.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.13 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-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, 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-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, 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-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
FortiFirewall	FFW-3980E, FFW-4200F, FFW-4400F, FFW-VM64, FFW-VM64-KVM
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 6.4.13. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2092.

FFW-1801F	is released on build 5459.
FFW-2600F	is released on build 5459.

FFW-4401F	is released on build 5459.
FG-400F	is released on build 5455.
FG-401F	is released on build 5455.
FG-600F	is released on build 5455.
FG-601F	is released on build 5455.

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 6.4.0 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 FG-VM64-AWSONDEMAND image is no longer provided. Both AWS PAYG and AWS BYOL models will share the same FG-VM64-AWS image for upgrading and new deployments. Remember to back up your configuration before upgrading.

Azure-On-Demand image

Bug ID	Description
657690	Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

FortiClient EMS Cloud registration

FortiOS 6.4.3 adds full support for FortiClient EMS Cloud service. Users will be able to register and use the service in mid-December 2020.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`, set the following to `block` in the SSL protocol settings:
  - in FortiOS 6.2.6 and later:

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl block
        end
    next
end
```

  - in FortiOS 6.4.3 and later:

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl-negotiation block
        end
    next
end
```

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 6.4.7.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 6.4.13 features.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description
792204	Update libssh2 to support DH parameters larger than 2048.
868164	Implement BIOS-level signature and file integrity checking for important system files and executables. Warn users of failed integrity checks, or prevent the system from booting depending on the severity and BIOS verification level. Kernel and userspace processes can also periodically verify the integrity of AV and IPS engine files, and other important system files and executables. FortiOS firmware and each release of an AV or IPS engine file are dually-signed by Fortinet CA and third-party CAs.

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*.

In 6.4.4, a new sub-option, *Delete*, was added when right-clicking on the device. This option is not available when the device is online, or the device is retrieved from FortiClient.

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

- FortiAnalyzer 6.4.12
- FortiManager 6.4.12
- FortiClient EMS 6.4.3 build 1600 or later
- FortiClient 6.4.3 build 1608 or later
- FortiAP 6.4.4 build 0456 or later
- FortiSwitch 6.4.5 build 0461 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. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC

13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.13. When Security Fabric is enabled in FortiOS 6.4.13, all FortiGate devices must be running FortiOS 6.4.13.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.13 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 6.4.13 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 6.4.13 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 6.4.13 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 6.4.13, 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 6.4.13.

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

Filtering facets are available for FortiView widgets in full screen and standalone mode.

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
```

WanOpt and web cache statistics

The statistics for WanOpt and web cache have moved from *Monitor* to a widget in *Dashboard*.

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
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Virtual WAN link member lost

The member of `virtual-wan-link` is lost after upgrade if the `mgmt` interface is set to `dedicated-to management` and part of an SD-WAN configuration before upgrade.

Enabling match-vip in firewall policies

As of FortiOS 6.4.3, `match-vip` is not allowed in firewall policies when the action is set to accept.

Hardware switch members configurable under system interface list

Starting in FortiOS 6.4.7, hardware switch members are also shown under `config system interface` with limited configuration options available.

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

Product integration and support

The following table lists FortiOS 6.4.13 product integration and support information:

Web Browsers	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 15. 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 15. 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**	• 6.4.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 15 and Fortinet Security Fabric upgrade on page 15. 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 6.0 and later are supported.
FortiClient iOS	• 6.4.0 and later
FortiClient Android and FortiClient VPN Android	• 6.4.0 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 0310 and later (needed for FSSO agent support OU in group filters) • Windows Server 2022 Standard • Windows Server 2022 Datacenter • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 4.2 version.
AV Engine	• 6.00176
IPS Engine	• 6.00160
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, 6.7, and 7.0

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 113 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Big Sur 11.4	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
iOS	Apple Safari

Operating System	Web Browser
	Mozilla Firefox 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 6.4.13. To inquire about a particular bug, please contact Customer Service & Support.

Explicit Proxy

Bug ID	Description
794124	HTTPS websites are not accessible if `certificate-inspection` is set in a proxy policy.
849794	Random websites are not accessible after upgrading when using a proxy policy.

Firewall

Bug ID	Description
727809	Disabled deny firewall policy with virtual server objects cannot be enabled after a firewall reboot.
739949	In HA virtual cluster scenario, the *Bytes* counter on the *Firewall Policy* page always shows *0 B* for the secondary while the *Edit Policy* page shows the correct *Total bytes* in the statistics.
808264	Stress test shows packet loss when testing with flow inspection mode and application control.
856187	Explicit FTPS stops working with IP pool after upgrading from 6.4.8 to 6.4.9.
865661	Standard and full ISDB sizes are not configurable on FG-101F.

GUI

Bug ID	Description
722358	When a FortiGate local administrator is assigned to more than two VDOMs and tries logging in to the GUI console, they get a command parse error when entering VDOM configuration mode.
748530	A gateway of *0.0.0.0* is not accepted in a policy route.
870675	CLI console in GUI reports *Connection lost.* when the administrator has more than 100 VDOMs assigned. **Workaround**: use SSH directly or reduce the number of VDOMs.

HA

Bug ID	Description
776355	Packet loss occurs on the software switch interface when a passive device goes down.
816883	High CPU usage on secondary device, and CPU lacks the AVX feature needed to load `libdpdk.so`.
830879	Running `execute ha manage 0 <remote_admin>` fails and displays a `Permission denied, please try again.` error if the 169.254.0.0/16 local subnet is not in the trusted host list.
832634	HA failovers occur due to the kernel hanging on FG-100F.
853900	The administrator `password-expire` calculation on the primary and secondary returns a one-second diff, and causes HA to be out-of-sync.
856643	FG-500E interface stops sending IPv6 RAs after upgrading.
874823	FGSP `session-sync-dev` ports do not use L2 Ethernet frames but always use UDP, which reduces the performance.

Intrusion Prevention

Bug ID	Description
715360	Each time an AV database update occurs (scheduled or manually triggered), the IPS engine restarts on the SLBC secondary blade.
775696	Each time an AV database update occurs (scheduled or manual), the IPS engine restarts on the SLBC secondary blade. This stops UTM analysis for sessions affected by that blade.
839170	IPS engine may crash (`SIGALRM`) when the system is busy because it might not receive enough run time.

IPsec VPN

Bug ID	Description
765174, 775279	Certain packets are causing IPsec tunnel drops on NP6XLite platforms after HA failover because the packet is not checked properly.
788751	IPsec VPN Interface shows incorrect TX/RX counter.
805301	Enabling NPU offloading in the phase 1 settings causes a complete traffic outage after a couple of ping packets pass through.

Bug ID	Description
822651	NP dropping packet in the incoming direction for SoC4 models.
840153	Unexpected dynamic selectors block traffic when `set mesh-selector-type subnet` is configured.
842528	Improper IKEv1 quick mode fragmentation from third-party client can cause an IKE crash.
877161	IPsec traffic failing from FortiGate with `Failed to find IPsec Common` error when dialup IPsec VPN tunnel has remote IP configured on the IPsec VPN interface.
892699	In an HA cluster, static routes via the IPsec tunnel interface are not inactive in the routing table when the tunnel is down.

Log & Report

Bug ID	Description
823183	FortiGates are showing *Logs Queued* in the GUI after a FortiAnalyzer reboot, even tough the queued logs were actually all uploaded to FortiAnalyzer and cleared when the connection restores.
873987	High memory usage from miglogd processes even without traffic.
874026	Caching a large number of service port entries causes high log daemon memory usage.

Proxy

Bug ID	Description
867614	Multiple and recurrent WAD crashes are causing platform instability and conserve mode after upgrading to 6.4.11 because the Unix stream might be null in some scenarios.

REST API

Bug ID	Description
745926	Using multiple logical AND symbols (&) on monitor API filtering causes a 502 Bad Gateway error.

Routing

Bug ID	Description
618684	When HA failover is performed to the other cluster member that is not able to reach the BFD neighbor, the BFD session is down as expected but the static route is present in the routing table.
769100	Policy routes order is changed after updating the source/destination of SD-WAN rules.
797590	GRE tunnel configured using a loopback interface is not working after changing the interface back and forth.
846107	IPv6 VRRP backup is sending RA, which causes routing issues.
860075	Traffic session is processed by a different SD-WAN rule and randomly times out.
862418	Application VWL crash occurs after FortiManager configuration push causes an SD-WAN related outage.
864626	FortiGate local traffic does not follow SD-WAN rules.
890379	After upgrading, SD-WAN is unable to fail over the traffic when one interface is down.

Security Fabric

Bug ID	Description
885810	The gcpd daemon constantly crashes (signal 11 segmentation fault).

SSL VPN

Bug ID	Description
781581	Customer internal website is not shown correctly in SSL VPN web mode.
803576	Comments in front of `<html>` tag are not handled well in HTML file in SSL VPN web mode.
803622	High CPU in SSL VPN once SAML is used with FortiAuthenticator and an LDAP server.
818196	SSL VPN does not work properly after reconnecting without authentication and a TX drop is found.
873995	Problem with the internal website using SSL VPN web mode.
850898	OS checklist for the SSL VPN in FortiOS does not include macOS Ventura (13).
884860	SSL VPN tunnel mode gets disconnected when SSL VPN web mode is disconnected by `limit-user-logins`.

Switch Controller

Bug ID	Description
798724	FortiSwitch exported ports in tenant VDOM are gone after rebooting the FortiGate.

System

Bug ID	Description
688009	Update built-in modem firmware that comes with the device in order for the SIM to be correctly identified and make LTE link work properly.
709679	Get `can not set mac address(16)` error message when setting a MAC address on an interface in HA that is already set.
721119	The forticron process uses high CPU.
729912	DNS proxy does not transfer the DNS query for IPv6 neighbor discovery (ND) when client devices are using random MAC addresses, so one device can configure many IPv6 addresses.
753421	Slow SNMP query performance of fgVpn2Tables OIDs when a large number of IPsec dialup tunnels are connected.
754681	The auto-script is not restarted when it is changed from HA synchronization.
766834	forticron allocates over 700 MB of memory, causes the FortiGate to go into conserve mode, and causes kernel panic due to 100 MB of configured CRL.
782962	PSU alarm log and SNMP trap are added for FG-10xF and FG-8xF models.
790656	DNS fails to correctly resolve hosts using the DNS database.
796094	Egress traffic on EMAC VLAN is using base MAC address instead.
800295	NTP server has intermittent unresolvable logs after upgrading to 6.4.
815937	FCLF8522P2BTLFTN transceiver is not working after upgrade.
828070	CLI displays `pipe() failed` error messages when sending the sensor value to SMC.
840960	When kernel debug level is set to `>=KERN_INFO` on NP6xLite platforms, some tuples missing debug messages may get flooded and cause the system to get stuck.
844937	FG-3700D unexpectedly reboots after the COMLog reported a kernel panic due to an IPv6 failure to set up the master session for the expectation session under some conditions.
850430	DHCP relay does not work properly with two DHCP relay servers configured.
850683	Console keeps displaying `bcm_nl.nr_request_drop ...` after the FortiGate reboots because of the `cfg-save revert` setting under `config system global`. Affected platforms: FG-10xF and FG-20xF.

Bug ID	Description
850688	FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs.
855151	There may be a race condition between the CMDB initializing and the customer language file loading, which causes the customer language file to be removed after upgrading.
859795	High CPU utilization occurs when relay is enabled on VLAN, and this prevents users from getting an IP from DHCP.
868002	FortiGate is unable to resolve DNS from the DNS database for local out traffic (ICMP and access to RADIUS server).

Upgrade

Bug ID	Description
743389	The `dnsfilter-profile` setting was purged from all DNS server entries upon upgrading from before 6.4.4.

User & Authentication

Bug ID	Description
679016, 749694	A fnbamd crash is caused when the LDAP server is unreachable.
688065	When using the `group-override-attr-type class` option in a RADIUS configuration, two extra characters are added at the end of the group name.
839801	FortiToken purge in a VDOM clears all FortiToken statuses in the system.
851233	FortiToken activation emails should include HTTPS links to documentation instead of HTTP.

VM

Bug ID	Description
785929	AWS FortiGate fails to bootstrap in new region of Cape Town, South Africa (af-south-1).

VoIP

Bug ID	Description
757477	PRACK will cause voipd crashes when the following conditions are met: `block-unknown` is disabled in the SIP profile, the PRACK message contains SDP, and PRACK fails to find any related previous transactions (this is not a usual case).

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
843324	FortiOS 6.4.13 is no longer vulnerable to the following CVE Reference: • CVE-2022-42472
858793	FortiOS 6.4.13 is no longer vulnerable to the following CVE Reference: • CVE-2022-43947
866013	FortiOS 6.4.13 is no longer vulnerable to the following CVE Reference: • CVE-2023-22641

Known issues

The following issues have been identified in version 6.4.13. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
877613	*Mark as Reject* can be still chosen as an *Action* in an *Anti-Spam Block/Allow List* in the GUI.

Anti Virus

Bug ID	Description
752420	If a .TAR.BZ2 or .TAR.GZ archive contains an archive bomb inside its compressed stream, the AV engine will time out.

Firewall

Bug ID	Description
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic. **Workaround**: rename the custom section to unique name between IPv4 and IPv6 policies.
770541	Within the *Policy & Objects* menu, the firewall, DoS, and traffic shaping policy pages take around five seconds to load when the FortiGate cannot reach the FortiGuard DNS servers. **Workaround**: set the DNS server to the FortiGuard DNS server.
843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI. This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.

Bug ID	Description

	Workaround: create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if `ALL` is the first firewall service in the list:
	`config firewall service custom`
	`edit "unused"`
	`set tcp-portrange 1`
	`next`
	`move "unused" before "ALL"`
	`end`

FortiView

Bug ID	Description
683654	FortiView pages with FortiAnalyzer source incorrectly display a *Failed to retrieve data* error on all VDOM views when there is a newly created VDOM that is not yet registered to FortiAnalyzer. The error should only show on the new VDOM view.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.
653952	*The web page cannot be found* is displayed when a dashboard ID no longer exists. **Workaround**: load another page in the navigation pane. Once loaded, load the original dashboard page (that displayed the error) again.
688016	GUI interface bandwidth widget does not show correct data for tunnel interface when ASIC offload is enabled on the firewall policy.
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI *Forward Traffic* log page can take time to load if there is no specific filter for the time range. **Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs.
743477	On the *Log & Report* > *Forward Traffic* page, filtering by the *Source* or *Destination* column with negation on the IP range does not work.

HA

Bug ID	Description
771999	Sessions not synchronized to HA secondary on an FGSP and FGCP combined setup.
779180	FGSP does not synchronize the `helper-pmap` expectation session.

Hyperscale

Bug ID	Description
734305	In the GUI, an FQDN or ISDB can be selected for a DoS policy, which is not supported (an error message appears). The CLI shows the correct options.
760560	The timestamp on the hyperscale SPU of a deny policy (policy id 0) is incorrect.
796368	Traffic shaping profile does not seem to have an effect on TCP/UDP traffic in hyperscale.
802369	Large client IP range makes fixed allocation usage relatively limited.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.
763736	IPS custom signature logging shows (even after being disabled) after upgrading to FortiOS 6.4.7.

Log & Report

Bug ID	Description
860822	When viewing logs on the *Log & Report* > *System Events* page, filtering by *domain\username* does not display matching entries. **Workaround**: use a double backslash (*domain\\username*) while filtering or searching by username only without the domain.

Proxy

Bug ID	Description
604681	WAD process with SoC SSL acceleration enabled consumes more memory usage over time, which may lead to conserve mode. **Workaround**: disable SoC SSL acceleration under the firewall SSL settings.

REST API

Bug ID	Description
759675	`Connection failed` error occurs on FortiGate when an interface is created and updated using the API in quick succession.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.

SSL VPN

Bug ID	Description
730416	Forward traffic log does not generate logs for HTTP and HTTPS services with SSL VPN web mode.

System

Bug ID	Description
555616	When NTurbo is enabled, it is unexpectedly provided with the wrong traffic direction information (from server or from client) to decide the destination for the data. This causes the traffic to be sent back to the port where it came from.
602141	The extender daemon crashes on Low Encryption (LENC) FortiGates.

Bug ID	Description
648085	Link status on peer device is not down when the admin port is down on the FortiGate.
664856	A VWP named .. can be created in the GUI, but it cannot be edited or deleted.
666664	Interface belonging to other VDOMs should be removed from interface list when configuring a GENEVE interface.
669645	VXLAN VNI interface cannot be used with a hardware switch.
685674	FortiGate did not restart after restoring the backup configuration via FortiManager after the following process: disable NPU offloading, change NGFW mode from profile-based to policy-based, retrieve configuration from FortiGate via FortiManager, and install the policy package via FortiManager.
751715	Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed.

Upgrade

Bug ID	Description
767808	The `asicdos` option for enabling/disabling NP6XLite DoS offloading is missing after upgrading to 6.4.9. Affected platforms: NP6XLite.
840921	When upgrading from 6.0.15 to 6.4.11, an existing explicit flow-based web filter profile changes to proxy-based.

User & Authentication

Bug ID	Description
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.

VM

Bug ID	Description
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
617046	FG-VMX manager not showing all the nodes deployed.
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).

Bug ID	Description
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
764392	Incorrect VMDK file size in the OVF file for hw13 and hw15. **Workaround**: manually correct the hw13 and hw15 OVF file's `ovf:size` value.

WiFi Controller

Bug ID	Description
662714	The `security-redirect-url` setting is missing when the `portal-type` is `auth-mac`.

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.