FortiOS - Release Notes

Version 6.4.1

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

July 21, 2020
FortiOS 6.4.1 Release Notes
01-641-625428-20200721

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-06-04	Initial release.
2020-06-05	Removed 565309, 584314, 610191, and 622812 from *Special notices*.
2020-06-17	Added 558685 to *Resolved issues*. Updated 638537 in *Known issues*.
2020-07-21	Renamed *Upgrade Information > SD-WAN zones* to *SD-WAN upgrade changes*. Updated *Upgrade Information > Fortinet Security Fabric upgrade*, *Upgrade Information > FortiView widgets*, *Upgrade Information > SD-WAN upgrade changes*, and *Product integration and support*.

Introduction and supported models

This guide provides release information for FortiOS 6.4.1 build 1637.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.1 supports the following models.

FortiGate	FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-61E, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-101E, 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 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 6.4.1 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.

Changes in CLI

Bug ID	Description

466868	The `vap-all` options for `wtp-profile` and `wtp` (with `override-vaps enabled`) have changed to `tunnel`, `bridge`, and `manual`.
	`config wireless-controller wtp-profile`
	`  edit FAP-Profile`
	`  config radio-1`
	`  set vap-all {tunnel | bridge | manual}`
	`  end`
	`  next`
	`end`
	The `wtp-mode` setting was removed from `config wireless-controller wtp`. The traffic mode for FortiAP, tunnel or bridge, is automatically determined by the SSID selection.

603846	Support DNS-over-TLS connections to FortiGuard secure DNS server. Options are only available when `fortiguard-anycast` is enabled.
	`config system fortiguard`
	`  set fortiguard-anycast enable`
	`  set fortiguard-anycast-source fortinet <==added`
	`  set anycast-sdns-server-ip 0.0.0.0 <==added`
	`  set anycast-sdns-server-port 853 <==added`
	`end`

605817	Add support for IBM Cloud SDN connector. FortiGates can define dynamic firewall addresses obtained from the IBM Cloud.
	`config system sdn-connector`
	`  edit <ibm-connector>`
	`  set type ibm <==added`
	`  set api-key <key>`
	`  set compute-generation <gen>`
	`  set ibm-region-gen1 <region>`
	`  next`
	`end`
	`config firewall address`
	`  edit <dynamic address>`
	`  set type dynamic`
	`  set sub-type sdn`
	`  set sdn <ibm-connector>`
	`  set filter <filter> <==added`
	`  next`
	`end`

Bug ID	Description

613730	Add `subscription-id` attribute for route table in Azure SDN configuration to allow route table updating in a different subscription.
	`config system sdn-connector`
	`edit "azsdn"`
	`config route-table`
	`edit "xxxxxxxxx-rtb1"`
	`set subscription-id "xxxxxxxxxxxxxxx" <==added`
	`set resource-group "xxxxxxxxx"`
	`config route`
	`edit "internal-forward"`
	`set next-hop "172.28.5.4"`
	`next`
	`end`
	`next`
	`end`
	`end`

616335	For VMware NSX SDN connector, add new CLI to support vCenter credentials so FortiGate can resolve NSX-T VMs and apply an NSX automation stitch to it.
	`config system sdn-connector`
	`edit <nsx server>`
	`set vcenter-server <server>`
	`set vcenter-username <username>`
	`set vcenter-password <password>`
	`next`
	`end`

625840	Add `diagnose system top-all` to show kernel process.

Changes in GUI behavior

Bug ID	Description
616294	When registering a device through the FortiGate GUI, a FortiCare registration disclaimer is displayed.
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.

Changes in default behavior

Bug ID	Description
537354	Interface egress shaping offload to NPU when `shaping-offload` is enabled.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
613155	Add two-factor authentication support to VPN IKEv2 for remote RADIUS and LDAP users.
618812	Populate source and destination user fields in traffic logs using RADIUS accounting information from authenticated RSSO users.
621046	FortiIPAM is a new IP address management service that helps manage IP addresses within a Security Fabric. FortiGates can use FortiIPAM to automatically assign IP addresses based on the configured network size for the FortiGate interface. The interface's DHCP server settings can be automatically configured to offer addresses within the same subnet.

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.

625063	In a scenario where transferring the device to another FortiCloud/FortiCare account is needed, users cannot do this directly on the FortiGate GUI if they have credentials to access to both accounts.
626075	Support *Signal Strength* and *Signal Strength/Noise* values by WiFi client IPs in the logs.
630238	Allow configuration of up to 16 FGSP standalone peers in `system standalone-cluster`.

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

- FortiAnalyzer 6.4.1
- FortiManager 6.4.1
- FortiClient EMS 6.4.0 build 1429
- FortiClient 6.4.1 build 1481
- FortiAP 6.4.0 build 416
- FortiSwitch 6.4.1 build 411

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.1. When Security Fabric is enabled in FortiOS 6.4.1, all FortiGate devices must be running FortiOS 6.4.1.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.1 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.4.1 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)

- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.4.1 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 6.4.1 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 6.4.1, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.4.1.

To configure `local-access` profile:

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

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

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

FortiGate VM with V-license

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

To enable `split-vdom`:

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

FortiGate VM firmware

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

Citrix 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
```

SD-WAN upgrade changes

- Renamed `virtual-wan-link` in `static route` to `sdwan`.

```
config router static
    edit 1
        set sdwan {enable | disable}
        ...
    next
end
```

- Added new table, `system.sdwan.zone`. Every SD-WAN member must be assigned to a zone. The default zone is `virtual-wan-link`.

```
config system sdwan
    config zone
        edit "vpn-zone"
        next
        edit "virtual-wan-link"
        next
    end
end
```

```
config system sdwan
    config members
        edit 1
            set interface "port1"
            set zone "vpn-zone"
        next
    end
end
```

- Upgrading will create individual SD-WAN zones for each SD-WAN member used in policies.
- When using SD-WAN zones in firewall policies, for `firewall.policy`, `firewall.policy6`, `firewall.proxy-policy`, and `firewall.security-policy`, the SD-WAN interfaces are changed to the zone name. Only SD-WAN zones can be used as `srcintf` and `dstintf`. Member interfaces of SD-WAN cannot be used directly.

```
config firewall policy
    edit 1
        set dstintf virtual-wan-link vpn-zone
        ...
    next
end
```

File filter as a standalone profile

The previously embedded file filter within web filter, email filter, SSH inspection, and CIFS has moved to a standalone profile. The file filter can be applied directly to firewall policies and supports various traffic protocols in proxy or flow mode.

```
config file-filter profile
    edit "test"
```

```
        set comment ''
        set feature-set flow
        set replacemsg-group ''
        set log enable
        set scan-archive-contents enable
        config rules
            edit "Block Exe"
                set comment ''
                set protocol http ftp smtp imap pop3 mapi cifs ssh
                set action block
                set direction any
                set password-protected any
                set file-type "exe"
            next
        end
    next
end
```

When upgrading to FortiOS 6.4.1, existing embedded file filter rules (web filter, email filter, SSH inspection, and CIFS) that are not used in any policies or profile groups will have new file filter profiles created for them. Any firewall policies, proxy policies, or profile groups with existing embedded file filter rules will have new file filter profiles created for them.

Product integration and support

The following table lists FortiOS 6.4.1 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 15. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 6.4.1 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 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**	• 6.2.0 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 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	• 6.00144
IPS Engine	• 6.00022
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 77 Google Chrome version 83
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 77 Google Chrome version 83
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Ubuntu 16.04 / 18.04	Mozilla Firefox version 54
OS X Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 77 Google Chrome version 83
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 6.4.1. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
582368	URL threat detection version show a large negative number after the FortiGate reboots.

Data Leak Prevention

Bug ID	Description
582480	scanunit crashes with signal 11 in dlpscan_mailheader when AV scans files via IMAP.
611513	DLP triggers scan unit watchdog timer and does not block the files.

Explicit Proxy

Bug ID	Description
617934	Web proxy should support forward server on TLS 1.3 certificate inspection connection.

Firewall

Bug ID	Description
622045	Traffic not matched by security policy when using service groups in NGFW policy mode.
622258	Move command in `firewall service category` does not work.

FortiView

Bug ID	Description
615524	*FortiView* > *All Sessions* should be supported as a standalone dashboard widget in navigation bar.

GUI

Bug ID	Description
401862	*Monitor* page display incorrect virtual server entries for IPv6, VIP46, and VIP64; right-clicking gives and error.
493819	Reorder function on *Authentication Rules* page does not work.
528145	BGP configuration gets applied on the wrong VDOM if user switches VDOM selection in between operations (slow GUI).
557786	GUI response is very slow when accessing *IPsec Monitor* (api/v2/monitor/vpn/ipsec is taking a long time).
564849	HA warning message remains after primary device takes back control.
589709	Status button in *Tunnel* column on *IPsec Tunnels* page should be removed.
592854	When editing a firewall address or address group created in the VPN wizard, invalid characters in the comments block submitting the change.
594702	When sorting the interface list by the *Name* column, the ports are not always in the correct order (port10 appears before port2).
601568	Interface status is not displayed on faceplate when viewed from *System* > *HA* page.
607549	GUI CMDB API to support case sensitive/insensitive filtering.
611857	Custom admin profile not showing logs as expected.
614056	Disabling the *Idle Logout* toggle on the *SSL-VPN Settings* page does not change the idle timeout setting, so the change does not persist after clicking *Apply*.
617937	Cannot add wildcard FQDN address into group in *Edit SSL/SSH Inspection Profile* page.
622510	Page gets stuck and message field is blank when doing policy lookup with a non-IP protocol.
623939	Interface bandwidth widgets for WAN, PPPoE and VDOM link interfaces are not loading.
624551	On POE devices, several sections of the GUI take over 15 seconds to fully load.
625747	Server certificate does not load into IPS after configuring SSL inspection profile in replace mode.
628373	Software switch members and their VLANs are not visible in the GUI interfaces list.
631734	GUI not displaying PoE total power budget on FOS 6.2.3.
634677	User group not visible in GUI when editing the user with a single right-click.

HA

Bug ID	Description
610324	HA sync has high CPU due to large number of IPv6 routes.
620093	Connectivity issue between Azure App and MySQL server. FortiGate is marking the SYN packet with ECN=CE flag.
621583	HA cannot display status in GUI when heartbeat cables reconnect.
621621	Ether-type HA cannot be changed.
623642	It takes up to 10 seconds to get NPU VDOM link up when rebooting primary unit.
626715	Out of sync issue caused by firewall address group member is either duplicated or out of order.

Intrusion Prevention

Bug ID	Description
622741	Traffic was blocked during the test with flow UTMs enabled.

IPsec VPN

Bug ID	Description
610558	ADVPN cannot establish after primary ISP has recovered from failure and traffic between spokes is dropped.
622506	L2TP over IPsec tunnel establishes but traffic cannot pass because wrong interface gets in route lookup.
623238	ADVPN shortcut cannot establish if both spokes are behind NAT.
631804	OCVPN errors showing in logs when OCVPN is disabled.
631968	IKE daemon signal 6 crash when `phase1 add-gw-route` is enabled.

Log & Report

Bug ID	Description
608187	Five fields (`devtype`, `devcategory`, `mastersrcmac`, `srcmac`, `srcserver`) are not included in the traffic log.
611778	FG-AWS unable to view log from FortiAnalyzer.
616485	Log ID 20114 missing in FGT_log_reference.xml and text.html.
622954	Inconsistent log output relating to the local-in policy.
628358	Logs are not generated in GUI and CLI after checking the file system (after power cable disconnected).

Proxy

Bug ID	Description
578850	Application WAD crash several times due to signal alarm.
601493	ISDB static route cannot be active for proxy policy.
612333	In FortiGate with squid configuration (proxy chain), get *ERR_SSL_PROTOCOL_ERROR* when using Google Chrome with certificate/deep inspection.
615791	Abbreviated handshake randomly receives `fatal illegal_parameter` against zendesk.com services/sites.
616577	WAD failed to do an error handling for bypass case.
617099	WAD crashes every few minutes.
617373	AV profiles block WSUS service.
619637	In transparent proxy policy with authentication on corporate firewall, it shows *Access Denied* after authentication.
620453	Application WAD crash several times due to signal alarm.
621787	Application WAD crash several times.
623108	FTP-TP reaches high memory usage and triggers conserve mode.
623213	Firewall does not handle 308 redirects properly for threat feed list.
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.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
580207	Policy route does not apply to local-out traffic.
608289	Make SD-WAN a security zone by itself.
616483	Policy route should not kick in for destination `exclude-member`.
617906	With multiple PPPoE links, local traffic to a link will cause RPF check fail if priority of the route is higher than the distance.
619343	Cannot ping old VRIPs when adding new VRIPs.
625345	The single BGP update message contains the same prefix in withdrawn routes and NLRI (advertised route).
626549	SD-WAN rules created using ISDB do not match/forward via the correct interface.
627901	`set dscp-forward` option is missing when using maximize bandwidth strategy in SD-WAN rule.
629521	SD-WAN IPv6 default route cannot be redistributed into BGP using `set default-originate-routemap6`.

Security Fabric

Bug ID	Description
609182	*Security Fabric Settings* page sometimes cannot load FortiSandbox URL threat detection version despite FortiSandbox being connected.
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.
623689	CSF branch FortiGate cannot successfully connect/verify certificate with remote EMS server.

SSL VPN

Bug ID	Description
556314	SSL VPN group bookmarks shown only for the first matched policy.
602480	Use jQuery to customize FortiGate SSL VPN log in page.

Bug ID	Description
604402	SSL VPN web access prompts for certificate authentication irrespective of realm.
607413	SMB/CIFS bookmark name gets scrambled if it contains special characters like space, backslash, colon, etc.
608453	Internal website is not accessible from SSL VPN due to some Sage X3 JS files with errors.
609358	Host check related settings should not be skipped when IPv6 tunnel mode is enabled.
610564	RDP over web mode SSL VPN to a Windows Server changes the time zone to GMT.
610905	SSL VPN bypassing logon count limit with different case in user name.
611190	SSL VPN SNI realm check does not work as expected when accessing non-specified SNI.
612540	SSL VPN web mode has problem accessing EPX website.
613612	Important GUI pages in 6.4.0 are not rendered well by SSL VPN portal.
615453	Web socket using socket.io could not be established through SSL VPN web mode.
616189	Cannot access, read, or download SharePoint 2019 or OneDrive documents; times out.
616429	Local user assigned with FortiToken cannot log in to SSL VPN web/tunnel mode when password change is required.
616879	Traffic cannot pass through FortiGate for SSL VPN web mode if the user is a PKI peer.
617170	https://outlook.office365.com cannot be accessed in SSL VPN web portal.
619296	FortiGate reverts default values of text on buttons in SSL VPN log on page.
619369	SSL VPN web mode has access problem for engage.leithaeusl website.
619914	Split-tunnel information is not recognized by legacy FortiClient SSL VPN Linux tool.
620221	File downloaded from SFTP server of SSL VPN portal is sometimes falsified.
621270	SSL VPN user groups are corrupted in auth list when the user is a member of more than 100 groups.
622068	Adding FQDN routing address in split tunnel configuration injects single route in client for multiple A records.
622871	SSL VPN web mode not displaying full customer webpage after logging in.
623231	Pages could not be shown after logging in to back-end application server.
624145	An internal website via SSL VPN web portal failed to load an external resource.
624197	SSL VPN web mode does not completely load the redirected corporate SSO page when accessing an internal resource.
624288	After SSL VPN proxy, one JS file runs with error.
624477	FortiClient SSL VPN split tunnel is not working from macOS Catalina.
624904	The Saudi Arabian Airlines website is not shown properly in SSL VPN web mode.

Bug ID	Description
625301	Riverbed SteelCentral AppResponse login form is not displaying in SSL VPN web mode.
625338	sslvpnd crashing with signal 7 on get_free_idx.
625554	SSL VPN connection was used when the DTLS UDP packet process failed and connection was destroyed.
626237	SAP portal link is not working in SSL VPN web mode.
626351	Online Excel file could not be displayed in SSL VPN web mode.
626816	In web mode, after entering the username/password in back-end application server, logging in, and waiting for a while, the URL automatically changes to a direct connection to the back-end.
627456	Traffic cannot pass when SAML user logs in to SSL VPN portal with group match.

Switch Controller

Bug ID	Description
613323	FortiSwitch trunk configuration sync issue after FortiGate failover.
622812	VLANs on a FortiLink interface configured to use a hardware switch interface may fail to come up after upgrading or rebooting.

System

Bug ID	Description
583472	When system is in an extremely high memory usage state (~90%), a power supply status `Power supply 1 AC is lost` might be mistakenly logged.
585053	NP6 VLAN LACP-based interface RX/TX counters not increasing.
589792	Secondary members of a redundant interface process frames creating duplicates when NP6 offload is enabled.
594871	Potential memory leak triggered by FTP command in WAD.
600560	SMC time has big drift after running a long time without rebooting.
610900	Low throughput on FG-2201E for traffic with ECN flag enabled.
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.
613136	Uninitialized variable that may potentially cause httpsd signal 6 and 11 crash issue.

Bug ID	Description
615168	Traffic with priority field fails to traverse NP6 shaper.
615435	Crashes might happen due to CMDB query allocation failure causing a segmentation fault.
615451	Empty VIP groups allowed when restoring a configuration file.
617154	Fortinet_CA is missing in FG-3400E.
617409	The FG-800D HA LED is off when HA status is normal.
619023	Proxy ARP configuration not loaded after interface shut/not shut.
619234	Purge policy is very slow when the number of policies is close to the maximum.
623113	FortiGate not entering A records in shadow DNS database for cross-subdomain CNAME requests.
625053	TCP SYN-ACK sent to different gateway when proxy-based UTM profiles are used.
628124	`source-ip` under `system fortiguard` is not taken for directregistration.fortinet.com when using *Register with FortiCare* window.
636069	Unable to handle kernel NULL pointer dereference at 000000000000008f.
630658	Auto-script output file size over 400 MB when configured output size is default 10 MB.

Upgrade

Bug ID	Description
615972	After upgrading from 6.2.2 to 6.2.3, the description field in the table has disappeared under DHCP reservation.

User & Authentication

Bug ID	Description
544035	Sessions authenticated by email time out by the policy timeout, which is much shorter than the timeout used by email/MAC authentication in the original pre-6.0 behavior.
591170	Sessions are removed from session table when FSSO group order is changed.
604906	FortiOS does not prompt for token when using RADIUS and two-factor authentication to connect to IPsec IKEv2.
605437	FortiOS does not understand CMPv2 `grantedWithMods` response.
609655	Captive portal exemption after upgrading the device from 6.2.2 to 6.2.3.
620097	Persistent sessions for de-authenticated users.

Bug ID	Description
620941	Two-factor authentication using FortiClient SSL VPN and FortiToken Cloud is not working due to push notification delay.
621161	src-vis crashes on receipt of certain ONVIF packets.
624328	Fix IoT daemon segfault crashes.
626532	fnbamd is not sending `Calling-Station-Id` in `Acces-Request` for L2TP/IPsec since 5.4.0.
627144	Remote admin LDAP user login has authentication failure when the same LDAP user has local two-factor authentication.

VM

Bug ID	Description
606527	GUI and CLI interface dropdown lists are inconsistent.
613730	Unable to update routing table for a resource group in a different subscription for Azure SDN.
622031	azd keeps crashing if Azure VM contains more than 15 tags.
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.

VoIP

Bug ID	Description
620742	RAS helper does not NAT the port 1720 in the `callSignalAddress` field of the `RegistrationRequest` packet sent from the endpoint.
630024	voipd crashes repeatedly.

Web Filter

Bug ID	Description
612217	Remove XOR from FortiGuard communications from URL filter, spam filter, and AV query.
616162	Custom replacement message is not shown when using web filter.

Bug ID	Description
616681	Separate file filter into its own profile.
618153	FSSO users cannot proceed on web filter warning page in flow-based inspection.
620803	Group name missing on web filter warning page in proxy-based inspection.
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.

WiFi Controller

Bug ID	Description
604853	Only the first `Fortinet-Group-Name` VSA is evaluated in authorized firewall WSSO users.
618456	High cw_acd usage upon polling a large number of wireless clients with REST API.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
558685	FortiOS 6.4.1 is no longer vulnerable to the following CVE Reference: • CVE-2020-12812

Known issues

The following issues have been identified in version 6.4.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
618718	`set certificate` configuration missing in `config endpoint-control fctems` after rebooting.

FortiView

Bug ID	Description
639109	*Top Countries/Regions by Bytes* widget keeps trying to load.

Log & Report

Bug ID	Description
637117	Incomplete log field returned from CEF formatted syslog message.

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
587824	Member of virtual WAN link lost after upgrade if management interface is `set dedicated-to management` before.

Upgrade

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

User & Authentication

Bug ID	Description
606327	FTM push return traffic (mobile device to FortiGate) has TLS handshake failure; same device with 6.2.3 GA is OK.

VM

Bug ID	Description
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).

WiFi Controller

Bug ID	Description
638537	*Applications*, *Destinations*, and *Policies* keep loading for *WiFi Clients* > *Diagnostics and Tools* drill-down.

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.