FortiOS - Release Notes

Version 6.4.5

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 27, 2023
FortiOS 6.4.5 Release Notes
01-645-687666-20230627

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-02-18	Initial release.
2021-02-23	Updated *Known issues* and *Resolved issues*.
2021-02-25	Removed *Built-in IPS engine* section. Updated *Known issues* and *Resolved issues*.
2021-03-01	Added 700356 to *Known issues*.
2021-03-03	Updated *Resolved issues*.
2021-03-22	Updated *New features or enhancements* and *Known issues*.
2021-03-31	Updated *Known issues* and *Resolved issues*.
2021-04-12	Updated *New features or enhancements* and *Known issues*.
2021-04-20	Updated *Known issues* and *Resolved issues*.
2021-04-28	Updated *Known issues*.
2021-05-10	Updated *Known issues*.
2021-05-17	Updated *Known issues*.
2021-05-31	Updated *Known issues* and *Resolved issues*.
2021-06-03	Updated FortiClient compatibility in *Product integration and support*.
2021-06-16	Updated *Known issues* and *Resolved issues*.
2021-06-28	Updated *Known issues*.
2021-07-05	Updated *Known issues*.
2021-07-12	Updated *Known issues*.
2021-07-16	Updated *Policy routing enhancements in the reply direction* in *Special notices*.
2021-08-09	Updated *Known issues*.
2021-08-12	Updated *Virtual WAN link member lost*.
2021-08-23	Updated *Known issues* and *Resolved issues*.
2021-09-07	Updated *Known issues*.
2021-09-21	Updated *Known issues*.
2021-10-04	Updated *Known issues*.
2021-10-20	Updated *Known issues*.

Date	Change Description
2021-11-01	Updated *Known issues* and *Resolved issues*.
2021-12-13	Updated *Known issues*.
2022-02-14	Updated *Fortinet Security Fabric upgrade* and *Product integration and support*.
2022-03-10	Updated *Known issues*.
2022-05-03	Updated *Product integration and support*.
2022-05-16	Updated *Known issues*.
2022-07-13	Updated *Known issues*.
2022-08-22	Updated *Known issues*.
2023-05-03	Updated *Known issues*.
2023-05-17	Updated *Known issues*.
2023-05-29	Updated *SSL traffic over TLS 1.0 will not be checked and will be bypassed by default*.
2023-06-14	Updated *Known issues*.
2023-06-27	Updated *Known issues* and *Resolved issues*.

Introduction and supported models

This guide provides release information for FortiOS 6.4.5 build 1828.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.5 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-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-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
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
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 6.4.5. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1828.

FG-80F	is released on build 5656.
FG-80F-BP	is released on build 5656.
FG-81F	is released on build 5656.
FG-100F	is released on build 5651.
FG-101F	is released on build 5651.
FG-200F	is released on build 5653.

FG-201F	is released on build 5653.
FGR-60F	is released on build 5654
FGR-60F-3G4G	is released on build 5654

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 and later adds full support for FortiClient EMS Cloud service.

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
    ```

Policy routing enhancements in the reply direction

When reply traffic enters the FortiGate, and a policy route or SD-WAN rule is configured, the egress interface is chosen as follows.

With `auxiliary-session enabled` in `config system settings`:

- Starting in 6.4.0, the reply traffic will not match any policy routes or SD-WAN rules to determine the egress interface and next hop.
- Prior to this change, the reply traffic will match policy routes or SD-WAN rules in order to determine the egress interface and next hop.

With `auxiliary-session disabled` in `config system settings`:

- The reply traffic will egress on the original incoming interface.

Changes in CLI

Bug ID	Description

640488	Add option to configure the maximum memory usage on the FortiGate's proxy for processing resources, such as block lists, allow lists, and external resources.
	`config system global`
	`    set proxy-resource-mode {enable | disable}`
	`end`

666855	FortiOS supports verifying client certificates with RSA-PSS series of signature algorithms, which causes problems with certain clients.
	Add attribute to control signature algorithms related to client authentication (only affects TLS 1.2):
	`config vpn ssl settings`
	`    set client-sigalgs {no-rsa-pss | all}`
	`end`

682561	Add command, `get system instance-id`.

Changes in default behavior

Bug ID	Description
598614	When a group and a `user-peer` is specified in an SSL VPN authentication rule, and the same group appears in multiple rules, each group and `user-peer` combination can be matched independently.
669018	Update link for Fortinet URL rating submission on web filter block/warning pages to point to https://globalurl.fortinet.net.
673609	The auto-join FortiCloud re-try timer has changed from 600 seconds to 60 seconds.

Changes in table size

Bug ID	Description
665668	Increase IPIP tunnel table size from 256 per VDOM and 512 globally to 1024 per VDOM and 1024 globally.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
658206	New REST API `POST /api/v2/monitor/vpn/ike/clear?mkey=<gateway_name>` will bring down IKE SAs tunnel the same way as `diagnose vpn ike gateway clear`.
660596	Because pre-standard POE devices are uncommon in the field, `poe-pre-standard-detection` is set to `disable` by default. Upgrading from previous builds will carry forward the configured value.
661105	By using `session-sync-dev` to offload session synchronization processing to the kernel (with various optimizations), four-member FGSP session synchronization can be supported to handle heavy loads.
667285	When configuring a NAC policy, it is sometimes useful to manually specify a MAC address to match the device. Wildcards in the MAC address are supported by specifying the * character.
673371	Support ICMP type 13 at local interface.

676484	When configuring the generic DDNS service provider as a DDNS server, the server type and address type can be set to IPv6. This allows the FortiGate to connect to an IPv6 DDNS server and provide the FortiGate's IPv6 interface address for updates.
	`config system ddns`
	`edit <name>`
	`set ddns-server genericDDNS`
	`set server-type {ipv4 | ipv6}`
	`set ddns-server-addr <address>`
	`set addr-type ipv6 {ipv4 | ipv6}`
	`set monitor-interface <port>`
	`next`
	`end`

677334	Add support for MacOS Big Sur 11.1 in SSL VPN OS check.
677684	In a hub and spoke SD-WAN topology with shortcuts created over ADVPN, a downed or recovered shortcut may affect which member is selected by an SD-WAN service strategy. The SD-WAN `hold-down-time` ensures that when a downed shortcut tunnel comes back up and the shortcut is added back into the service strategy equation, the shortcut is held to low priority until the `hold-down-time` has passed.
680599	Increase the ICMP rate limit to allow more ICMP error message to be sent by the FortiGate per second. The ICMP rate limit has changed from 1 second (100 jiffies) to 10 milliseconds (1 jiffy).
690179	The SD-WAN REST API for health check and SLA log now exposes ADVPN shortcut information in its result. The `child_intf` attribute returns the statistics for the corresponding shortcuts. A CLI command is also added to display real-time SLA information for ADVPN shortcuts. `# diagnose sys sdwan sla-log <health check name> <sequence number> <child name>`

Bug ID	Description
691411	Ensure EMS logs are recorded for dynamic address related events under *Log & Report* > *Events* > *SDN Connector Events* logs: • Add EMS tag • Update EMS tag • Remove EMS tag
697675	Increase the maximum number of managed FortiSwitches from 8 to 16.

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

- FortiAnalyzer 6.4.4
- FortiManager 6.4.4
- FortiClient EMS 6.4.1 build 1498 or later
- FortiClient 6.4.1 build 1519 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. 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 6.4.5. When Security Fabric is enabled in FortiOS 6.4.5, all FortiGate devices must be running FortiOS 6.4.5.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.5 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 6.4.5 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 6.4.5 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 6.4.5 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 6.4.5, 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 6.4.5.

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, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *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.

Product integration and support

The following table lists FortiOS 6.4.5 product integration and support information:

Web Browsers	• Microsoft Edge 88 • Mozilla Firefox version 85 • Google Chrome version 88 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. 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**	• 6.4.0 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 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 0295 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 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	• 6.00154
IPS Engine	• 6.00071
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
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 85 Google Chrome version 88
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 85 Google Chrome version 88
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 68
macOS Big Sur 11.0	Apple Safari version 14 Mozilla Firefox version 85 Google Chrome version 88
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 6.4.5. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
524571	Quarantined files cannot be fetched in the AV log page if the file was already quarantined under another protocol.

Application Control

Bug ID	Description
576727	*Unknown Applications* category is not present in NGFW policy-based mode.

DNS Filter

Bug ID	Description
674302	Do not send FortiGate generated DNS response if no server response was received and redirect DNS queries time out.

Explicit Proxy

Bug ID	Description
642196	Web proxy forwarding server health check does not send user name and password.
664380	When configuring explicit proxy with forward server, if `ssl-ssh-profile` is enabled in `proxy-policy`, WAD is unable to correctly learn the destination type correctly, so the destination port is set to 0, but the squid proxy server does not accept the request and returns an error.

Firewall

Bug ID	Description
661014	FortiCarrier has GTP dropped packet log after configuring GTP allow list.
663062	Sessions are marked dirty when IPsec dialup client connects/disconnects and policy routes are used.
665964	In NAT64 scenario, ICMPv6 `Packet too big` message translated to ICMPv4 does not set the MTU/DF bit correctly.
667772	When NGFW mode is set to policy mode and a security policy is configured, the Quard daemon should start when either an anti-virus, web filter, application, IPS, or DLP profile is enabled.
675353	Security policy (NGFW mode) flow-based UTM logs are still generated when policy traffic log is disabled.
675772	Virtual wire pair of mirror traffic on FortiOS 6.4 cannot detect IPS attacks because of failed anti-replay checks.
675823	In NGFW mode, traffic is not passing through zone members when intra-zone traffic is allowed.
678813	Cannot change the order of IPv4 access control list entries from FortiOS after upgrading from 6.4.1. to 6.4.3.
682956	ISDB is empty/crashes after upgrading from 6.2.4/6.2.5 to 6.2.6.
683604	When changing a policy and creating a firewall sniffer concurrently, there is traffic that is unrelated to the policy that is being changed and matching the implicit deny policy. Some IPv4 firewall policies were missing after the change.

FortiView

Bug ID	Description
628225	FortiView *Compromised Hosts* dashboard cannot show data if FortiAnalyzer is configured using the FQDN address in the log setting. FortiAnalyzer configured with an IP address does not have this issue.
673225	FortiView *Top Traffic Shaping* widget does not show data for outbound traffic if the source interface's role is WAN. Data is displayed if the source interface's role is LAN, DMZ, or undefined.
673478	Some FortiView graphs and drilldown views show empty data due to filtering issue. Affected graphs/views: *Top System Events*, *Top Authentication Failures*, *Policy View*, and *Compromised Host View*.
683413	Some FortiView pages/widgets fail to query data from FortiAnalyzer Cloud if the local FortiAnalyzer is not enabled.

Bug ID	Description
	Affected pages/widgets: *Compromised Hosts*, *FortiView Cloud Applications*, *FortiView VPN*, *FortiView Web Categories*, *Top Admin Logins*, *Top Endpoint Vulnerabilities*, *Top Failed Authentication*, *Top System Events*, *Top Threats*, *Top Threats - WAN*, and *Top Vulnerable Endpoint Devices*.

GUI

Bug ID	Description
561420	On *Traffic Shaping Policy* list page, right-click option to show matching logs does not work.
589749	Incorrect error message on log settings page, *Connectivity issue, 0 logs queued*, for FortiAnalyzer connection when the VDOM is in transparent mode with log setting override enabled.
592854	An address created by the VPN wizard cannot save changes due to an incorrect validation check for parentheses, *()*, in the *Comments* field.
602102	Warning message is not displayed when a user configures an interface with a static IP address that is already in use.
636208	On *SD-WAN Rules* page, the GUI does not indicate which outgoing interface is active. This is due to auto-discovery VPN routing changes.
652522	When performed from the primary FortiGate, using the GUI to change a firewall policy action from accept to deny does not disable the IP pool setting, causing the HA cluster to be out of sync. Updating the policy via the CLI does not have this issue.
654705	Aggregated IPsec VPN interface shows as down when each member tunnel has phase 1 and phase 2 names that differ from each other.
656668	On the *System* > *HA* page, GUI tooltip for the reserved management interface incorrectly shows the connecting IP address instead of the configured IP address.
659490	A remote certificate in VDOM mode that has no references cannot be deleted from the GUI. Removal is possible using the CLI.
662705	REST API, `api/v2/monitor/firewall/internet-service-details`, returns `start_ip` and `end_ip` in raw format instead of string format.
664007	GUI incorrectly displays the warning, *Botnet package update unavailable, AntiVirus subscription not found.*, when the antivirus entitlement is expiring within 30 days. The actual Botnet package update still works within the active entitlement duration.
665111	There is no way to add a line break when using the GUI to edit the replacement message for *pre_admin-disclaimer-text*. One must use the CLI with the `Shift + Enter` keys to insert a line break.
665712	When multiple favorite menus are configured, the new features video pops up after each GUI login, even though user previously selected *Don't show again*.

Bug ID	Description
666999	When editing the *Poll Active Directory Server* page, the configured LDAP server saved in FSSO polling is not displayed. Users must use the CLI to modify the setting.
668470	FortiGuard DDNS setting incorrectly displays truncated unique location and empty server selection after saving changes.
670026	When editing a DoS policy, users were able to click *OK* twice as there was a small delay until the dialog was saved and closed. Clicking twice would cause unwanted changes to the policy. This has been corrected as *Submit* buttons are now disabled while a dialog is submitting. This fix covers all policy dialogs.
672599	After performing a search on firewall *Addresses*, the matched count over total count displayed for each address type shows an incorrect total count number. The search functionality still works correctly.
673496	When editing phase 2 configurations, clicking *Complete Section* results in a red highlight around the phase 2 configuration GUI box, and users cannot click *OK* to save configuration changes.
676165	Script pushed from FortiManager 6.4.2 to FortiOS 6.4.2 to add address objects and an address group only pushes the address group.
680805	The list of firewall schedules displays time based on the browser time, even though the global time preference is set to use the FortiGate system time. The *Edit Schedule* page does not have this issue.
682008	On the *SSL-VPN Settings* page, the option to send an SSL VPN configuration to a user for FortiClient provisioning does not support showing domain name for VPN gateway.
682077	Log viewer should use relative timestamps for dates less than seven days old.
682440	On *Firewall Policy* list, the tooltip for *IP Pool* incorrectly shows *Port Block Allocation* as being exhausted if there are expiring PBAs available to be reallocated.
684076	Erroneous duplication error displayed when creating a phase 2 with *Named IPv6 Address* set to *all* if there is already a phase 2 entry defined with *Named IPv4 Address* set to *all*. The CLI must be used for this configuration.
684904	When a FortiGate with VDOM and explicit proxy enabled has an access profile with packet capture set to none, administrators with this access profile are not able to create an explicit proxy policy.
688076	The *Firewall Address* and *Service* pages cannot load on a downstream FortiGate if *Fabric Synchronization* is enabled, but the downstream FortiGate cannot reach the root FortiGate.
688994	The *Edit Web Filter Profile* page incorrectly shows that a URL filter is configured (even though it is not) if the URL filter entry has the same name as the web filter profile in the CLI.
689605	On some browser versions, the GUI displays a blank dialog when creating custom application or IPS signatures. Affected browsers: Firefox 85.0, Microsoft Edge 88.0, and Chrome 88.0.

HA

Bug ID	Description
540600	The HA `hello-holddown` value is divided by 10 in the hatalk daemon, which makes the `hello-holddown` time 10 times less than the configuration.
670331	Management access not working in transparent mode cluster after upgrade.
675781	HA cluster goes out of sync with new custom DDNS entry, and changes with respect to the `ddns-key` value.
678309	Cluster is out of sync because of `config vpn certificate ca` after upgrade.
684051	IPv6 link local address is not generated in FGCP.

Intrusion Prevention

Bug ID	Description
654307	Incorrect direction and banned location by quarantine action for `ICMP.Oversized.Packet` signature in NGFW policy mode.
668631	IPS is constantly crashing, and ipshelper has high CPU when IPS extended database has too many rules (more than 256) sharing the same pattern. Affected models: SoC3-based FortiGates.

IPsec VPN

Bug ID	Description
642543	IPsec did not rekey when keylife expired after back-to-back HA failover.
652774	OCVPN spoke-to-spoke communication intermittently fails with mixed topology where some spokes have two ISPs and some have one, but the hubs have two.
655895	Unable to route traffic to a spoke VPN site from the hub FortiGate when the dialup IPsec VPN interface is dual stacked (IPv4/IPv6).
670025	IKEv2 `fragmentation-mtu` option is not respected when EAP is used for authentication.
675838	iked ignores phase 1 configuration changes due to frequent FortiExtender cmdb changes.
678166	TFTP upload not working when application control and ASIC offload are enabled.
678800	Kernel may crash on link event update with `net-device` enabled.
687749	iked HA sync crashed on secondary with authenticated user group in firewall policy. Affected models: all except NP7 platforms (FG-180xF, FG-260xF, FG-420xF, FG-440xF).

Log & Report

Bug ID	Description
650886	No log entry is generated for SSL VPN login attempts where two factor authentication challenge times out.
654363	Traffic log shows *Policy violation* for traffic hitting the allow policy in NGFW policy mode.
667274	FortiGate does not have log disk auto scan failure status log.
667950	IPS UTM log is missing `msg=` and `attackcontext=` TLV fields because the TLV buffer is full and not sent to miglogd.
675347	When searching for some rarely-found logs within a large volume of logs, there is a long period of time before the results are returned. During the waiting period, if any new requests arrive, the old search session cannot be cleared. There is then a risk that multiple processes exist together, which may cause performance issues.
682374	Traffic logs not forwarded correctly to syslog server in CEF format.

Proxy

Bug ID	Description
640488, 669736, 675480	When URLs for block/allow/external resource are processed, the system might enter conserve mode when external resources are very big.
658257	StartTLS-SMTP traffic gets blocked by the firewall when certificate inspection (proxy mode) and the IPS sensor are enabled in a policy.
664737	WAD crash with signal 11 (`/bin/wad => wad_ui_diag_session_get`).
675343	WAD crashes with transparent web proxy when connecting to a forward server.
675525	No WAD sessions displayed when running `diagnose wad filter`.
680651	Memory leak when retrieving the thumbnailPhoto information from the LDAP server.
681134	Proxy-based SSL certification inspection session hangs if the outbound probe connection has no routes.
682002	An incorrect teardown logic on the WAD SSL port causes memory leak.
688006	WAD user information daemon crashes on purging extra interfaces that exist in multiple VDOMs.
692462	Transparent proxy implicit deny policy is not blocking access.

REST API

Bug ID	Description
597707	REST API `/api/v2/monitor/firewall/security-policy` adds UUID data for security policy statistics.
658206	New REST API `POST /api/v2/monitor/vpn/ike/clear?mkey=<gateway_name>` will bring down IKE SAs tunnel the same way as `diagnose vpn ike gateway clear`.
663441	REST API unable to change status of interface when VDOMs are enabled.

Routing

Bug ID	Description
672061	In IPsec topology with hub and ~1000 spokes, hundreds of spoke tunnels are flapping, causing BGP instability for other spokes.
677928	SD-WAN with `sit-tunnel` as a member creates an unwanted default route.
680365	BGP is choosing local route that should have been removed from the BGP network table.
687034	bgpd memory leak if running BGP on 6.2.7 and 6.4.4.
692241	BGP daemon consumes high CPU in ADVPN setup when disconnecting after socket writing error.

Security Fabric

Bug ID	Description
650724	Invalid license data supplied by FortiGuard/FortiCare causes invalid warning in the *Security Rating* report.
673560	Compromised host automation stitch with IP ban action in multi-VDOM setup always bans the IP in the root VDOM.

SSL VPN

Bug ID	Description
598614	When a group and a `user-peer` is specified in an SSL VPN authentication rule, and the same group appears in multiple rules, each group and `user-peer` combination can be matched independently.
623379	Memory corruption in some DNS callback cases causes SSL VPN crash.
630068	When sslvpn SSH times-out, a crash is observed when the SSH client is empty.
656557	The map on the http://www.op***.org website could not be shown in SSL VPN web mode.
663723	SSL VPN with user certificate and credential verification allows a user to connect with a certificate signed by a trusted CA that does not match the certificate chain of the configured CA in the user peer configuration.
666513	An internal web site via SSL VPN web mode, https://***.46.19.****:10443, is unable to open.
666855	FortiOS supports verifying client certificates with RSA-PSS series of signature algorithms, which causes problems with certain clients.
669506	SSL VPN web mode cannot load web page https://jira.ca.ob***.com properly based on Jira application.
669900	SSL VPN crash when updating the existing connection at the authentication stage.
673320	Pop-up window does not load correctly when accessing internal application at https://re***.wo***.nl using SSL VPN web mode.
674279	Customer cannot access SAP web GUI with SSL VPN bookmark.
675196	RTA login webpage is not displaying in SSL VPN web mode.
675901	Internal website https://po***.we***.ac.uk is not loading correctly with SSL VPN bookmark.
677256	Custom languages do not work in SSL VPN web portals.
677550	GUI issues on the internal Atlassian Jira web portal in SSL VPN web mode.
678130	Customer internal website, https://va***.do***.com:21108/mne, cannot be displayed correctly in SSL VPN web mode.
678132	SSL VPN web portal SSO credentials for alternative option are not working.
678450	Unable to view the management GUI of PaloAlto running on 8.1.16 in SSL VPN web mode.
681626	Internal Gridbees portal does not display in SSL VPN web mode.
684012	SSL VPN crashed with signal 11 (segmentation fault) `uri_search` because of rules set for a special case.
685269	SSL VPN web mode is not working properly for aw***.co***.com website.
685854	After SSL VPN proxy rewrite, some Salto JS files could not run.

Switch Controller

Bug ID	Description
686031	LLDP updates from FortiSwitch can cause flcfgd to leak memory.

System

Bug ID	Description
598464	Rebooting FG-1500D in 5.6.x during upgrade causes an L2 loop on the heartbeat interface and VLAN is disabled on the switch side.
628642	Issue when packets from the same session are forwarded to each LACP member when NPx offloading is enabled.
648083	cmdbsvr may crash with signal 11 (segmentation fault) when frequently changing firewall policies.
649937	The `diagnose geoip geoip-query` command fails when `fortiguard-anycast` is disabled.
651103	FG-101F crashed and rebooted when adding `vlan-protocol 8021ad` VLAN.
654131	No statistics for TX and RX counters for VLAN interfaces.
665332	When VDOM has large number of VIPs and policies, any firewall policy change causes cmdbsvr to be too busy and consume high CPU.
665550	Fragmented UDP traffic does not assemble on the FortiGate and does not forward out.
667722	VLAN interface created on top of a 10 GB interface is not showing the actual TX/RX counters.
667962	httpsd crashed and `*** signal 6 (Aborted) received ***` appears when loading configurations through REST API with interactions.
669914	No statistics for TX and RX counters for VLAN interfaces.
669951	confsyncd may crash when there is an error parsing through the internet service database, but no error is returned.
670897	Update GTP code to be compatible with newer versions (GTPv1 and GTPv2).
670962	Packet loss occurs when traffic flow between VLAN interfaces is created under 10G LACP link.
671643	NTurbo does not work when enabled in IPsec tunnel or with session helper.
673609	The auto-join FortiCloud re-try timer 600 second value is too large.
675171	L2TP with status set to enable should be configured before EIP and SIP.
675508	When provisioning a FortiGate and FortiSwitch with enforced firmware version 6.4.2 in FortiManager, the physical port for FortiLink is down and cannot connect to FortiSwitch.

Bug ID	Description
679114	DHCP discover request is wrongly forwarded to all IPsec VPN interfaces when tunnel flipping occurs.
687519	Bulk changes through the CLI are very slow with 24000 existing policies.
695252	FortiExtender VLAN interface cannot get updated LTE IP.

User & Authentication

Bug ID	Description
658228	The authd and foauthd processes may crash due to crypto functions being set twice.
666857	LDAP connectivity delays in transparent mode VDOM.
667025	FortiGate does not send LLDP PDU when it receives LLDP packets from VoIP phones.
664123	Log enrichment for source and destination IP with RSSO user information in logs not properly working for IPv4 with framed route attribute in RADIUS accounting.
675226	The `ssl-ocsp-source-ip` setting not configurable in non-management VDOMs.
675539	FSSO collector status is down, despite that it is reported as connected by authd in a multi-VDOM environment.
682966	FortiGate is unable to parse IPv6 RADIUS accounting packet (`Parse error: IP6 Prefix`).

VM

Bug ID	Description
620654	Spoke dialup IPsec VPN does not initiate connection to hub after FG-VM HA failover in Azure.
646161	FG-VM8 does not recognize all memory allocated in Hyper-V.
669722	Unable to import more than 50 groups from NSX-T SDN connector.
672509	OCI HA unable to handle cross-compartment failover.
682260	After enabling DPDK, the FG-VM license becomes invalid. After rebooting, the license becomes valid again.
682420	Dialup IPsec tunnel from Azure may not be re-established after HA failover.
682561	`get system status` output can be stuck getting the instance ID.
689307	HA secondary VMSL license is invalid after reboot.
690863	EIP is not updating properly with `execute update-eip` command in Azure with standard SKU public IP in some Canadian regions, like CanadaCentral and CanadaEast.

Web Filter

Bug ID	Description
668325	A hanging FortiGuard connection is not torn down in some situations.
669018	Change URL re-evaluation link on web filter block pages to HTTPS.
675436	YouTube channel home page on blocklist is not blocked when directed from a YouTube search result.
676403	Replacement message pictures (FortiGuard web filter) are not displayed in Chrome.
678467	Safe search URL option is not working while the original query in Google Images has the same parameter name.

WiFi Controller

Bug ID	Description
620764	AP country and region settings are not updating as expected.
625630	FWF-60E hangs with looping kernel panic at WiFi driver.
672136	Log severity for wireless events in FortiWiFi and FortiAP should be reconsidered for CAPWAP teardown.
676640	cw_acd crash with `*** signal 8 (Floating point exception) received ***` after upgrading to 6.4.3.

Known issues

The following issues have been identified in version 6.4.5. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

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
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed. **Workaround**: clear the session after policy change.
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.

FortiView

Bug ID	Description
621453	FortiGate cannot get detailed information on FortiClient vulnerabilities from FortiAnalyzer.
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
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches. This performance issue needs a fix on both FortiOS and FortiSwitch. A fix was provided in FortiOS 7.0.1 GA and FortiSwitch 7.0.1 GA.
645158	When logging into the GUI via FortiAuthenticator with two-factor authentication, the FortiToken Mobile push notification is not sent until the user clicks *Login*.
674592	When `config ha-mgmt-interfaces` is configured, the GUI incorrectly shows an error when setting overlapping IP address.
688016	GUI interface bandwidth widget does not show correct data for tunnel interface when ASIC offload is enabled on the firewall policy.
695815	When editing the external connector *Poll Active Directory Server* from the GUI, the *Users/Groups* option is always an empty value, even if there is an existing group configured. **Workaround**: manage the option in the CLI.
697482	If FortiGate Cloud is not activated, users cannot edit the *Log Settings* page from the GUI. Affected models: FG-200F and FG-201F.
699508	When an administrator ends a session by closing the browser, the administrator timeout event is not logged until the next time the administrator logs in.
701742	Items added to *Favorites* are lost after a logout or reboot.
702065	After upgrading to 6.4.4, the RADIUS server with non-FortiToken two-factor authentication does not work in the GUI.
704618	When login banner is enabled, and a user is forced to re-login to the GUI (due to password enforcement or VDOM enablement), users may see a *Bad gateway error* and HTTPSD crash. **Workaround**: refresh the browser.
713529	When a FortiGate is managed by FortiManager with FortiWLM configured, the HTTPS daemon may crash while processing some FortiWLM API requests. There is no apparent impact on the GUI operation.
745998	An IPsec phase 1 interface with a name that contains a `/` cannot be deleted from the GUI. The CLI must be used.
763925	GUI shows user as expired after entering a comment in guest management.

IPsec VPN

Bug ID	Description
691929	When multiple dialup phase 1 gateways are configured on the hub that are nearly identical, when using peer group authentication after `fnbam` verification, the IKE gateway could switch from one to another even if two gateways have a different network ID.

Log & Report

Bug ID	Description
661040	Cyrillic characters not displayed properly in local reports.
677540	First TCP connection to syslog server is not stable.

Proxy

Bug ID	Description
684168	WAD process consumes memory and crashes because of a memory leak that happened due to a coding error when calling the FortiAP API. The API misbehaves when there are no FortiAP appliances in the cluster.
695042	A coding error can cause integer overflow on crafted HTTP requests and read out-of-boundary memory. Sometimes, PCRE match crashes due to this out-of-boundary memory access.
714109	YouTube server added new URLs (`youtubei/v1/player`, `youtubei/v1/navigator`) that caused proxy option to restrict YouTube access to not work.
709623	WAD crashes seen in user information upon user purge and during signal handling of user information history.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.

REST API

Bug ID	Description
713445	For API user tokens with CORS enabled and set to wildcard *, direct API requests using this token are not processed properly. This issue impacts FortiOS version 5.6.1 and later. **Workaround**: set CORS to an explicit domain.
714075	When CORS is enabled for REST API administrators, POST and PUT requests with body data do not work with CORS due to the pre-flight requests being handled incorrectly. This only impacts newer browser versions that use pre-flight requests.

Routing

Bug ID	Description
686829	ADVPN and SD-WAN reply direction randomly chooses ECMP path rather than following shortcut.
691687	Return packets are not always sent back through the correct path.
693238	OSPF neighbor cannot form with spoke in ADVPN setup if the interface has a parent link and it is a tunnel.
703782	Traffic to FortiToken Mobile push server does not follow SD-WAN/PBR rules.
704225, 706448	In some WAD proxy cases, the WAD local session cannot get the SYN-ACK packet.
705470	Reply direction keeps flapping between different tunnels after unrelated FIB update.
706417	FortiGate crashes when doing `ping6` on VDOM link interface.
712093	Hub return path does not update after branch SD-WAN SLA failover.

Security Fabric

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

SSL VPN

Bug ID	Description
718133	In some conditions, the web mode JavaScript parser will encounter an infinite loop that will cause SSL VPN crashes.

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.
568399	FG-200E has `np6lite_lacp_lifc` error message when booting up a device if there are more than seven groups of LAGs configured.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
648085	Link status on peer device is not down when the admin port is down on the FG-500E.
666664	Interface belonging to other VDOMs should be removed from interface list when configuring a GENEVE interface.
672183	UDP 4500 inter-VDOM traffic is not offloaded, causing BFD/IPsec to drop.
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.
705734	FWF-40F has random kernel panic with 6.4.4 firmware.

Upgrade

Bug ID	Description
725369	After upgrading to 6.4.5, VIP randomly stops working and a `find DNAT: IP-0.0.0.0` message appears.

User & Authentication

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW.
682394	FortiGate is unable to verify the CA chain of the FSSO server if the chain is not directly rooted to FSSO endpoint.

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).
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
722290	Azure slow path NetVSC SoftNIC has stuck RX. If using an IPsec tunnel, use UDP/4500 for ESP protocol (instead of IP/50) when SR-IOV is enabled. On the phase 1 interface, use `set nattraversal forced`. UDP/4500 is the fast path for Azure SDN, and IP/50 is the slow path that stresses guest VMs and hypervisors to the extreme. If using cross-site IPsec data backup, use Azure VNet peering technology to build raw connectivity across the site, rather than using the default IP routing based on the assigned global IP address.

WiFi Controller

Bug ID	Description
662714	The `security-redirect-url` setting is missing when the `portal-type` is `auth-mac`.
677994	Newly discovered and authorized FortiAP will cause HA sync issue. On the HA secondary member, if the WTP profile has a radio in monitor mode, it will be changed to AP mode and unset the band.

698961	FWF-60F/61F and FWF-40F encounters kernel panic (`LR is at capwap_find_sta_by_mac`) when one managed FortiAP is authenticating WiFi clients.
	Workaround: disable CAPWAP offloading, then reboot for the change to take effect.
	`config system npu`
	`    set capwap-offload disable`
	`end`

Bug ID	Description
709871	After the firmware upgrade, the AP cannot register to the central WLC because NPU offload changed the source and destination ports from 4500 to 0.

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.