FortiOS - Release Notes

Version 6.4.6

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

NSE 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

December 13, 2021
FortiOS 6.4.6 Release Notes
01-646-710382-20211213

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-05-20	Initial release.
2021-05-25	Updated *Known issues* and *Resolved issues*.
2021-06-03	Updated FortiClient compatibility in *Product integration and support*.
2021-06-16	Added *Built-in AV engine* and *Built-in IPS engine*. Updated *New features or enhancements*, *Known issues*, and *Resolved issues*.
2021-06-28	Updated *Built-in AV engine* and *Known issues*.
2021-07-12	Updated *Special branch supported models*, *Built-in IPS engine*, *Known issues*, *Resolved issues*, and *Product integration and support*.
2021-07-16	Updated *Policy routing enhancements in the reply direction* in *Special notices*.
2021-07-26	Updated *New features or enhancements*, *Known issues*, and *Resolved issues*.
2021-07-27	Updated *Known issues*.
2021-07-29	Updated *Known issues*.
2021-08-09	Updated *Known issues*.
2021-08-11	Updated *Built-in IPS engine* and *Known issues*.
2021-08-12	Updated *Virtual WAN link member lost*.
2021-08-23	Updated *Known issues* and *Resolved issues*.
2021-08-24	Updated *Resolved issues*.
2021-09-07	Updated *Known issues*, *Resolved issues*, and *Built-in AV engine*.
2021-09-21	Updated *New features or enhancements* and *Known issues*.
2021-10-01	Updated *Special branch supported models*.
2021-10-04	Updated *Known issues*.
2021-10-20	Updated *Known issues*, *Resolved issues*, and *Built-in IPS engine*.
2021-11-01	Updated *Known issues* and *Resolved issues*.
2021-11-04	Added *Part numbers of supported FG-10xF Generation 2 models* in *Special notices*.
2021-11-15	Updated *Known issues*.
2021-11-29	Updated *Known issues*.
2021-12-06	Updated *Changes in CLI* and *Resolved issues*.
2021-12-13	Updated *Known issues* and *Resolved issues*.

Introduction and supported models

This guide provides release information for FortiOS 6.4.6 build 1879.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.6 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-81E, FG-81E-POE, FG-81F, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-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 Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
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 6.4.6. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1879.

FG-200F	is released on build 5785.
FG-201F	is released on build 5785.
FG-1800F	is released on build 5868.
FG-1801F	is released on build 5868.
FG-2600F	is released on build 5868.

FG-2601F	is released on build 5868.
FG-3500F	is released on build 6135.
FG-3501F	is released on build 6135.
FG-4200F	is released on build 5868.
FG-4201F	is released on build 5868.
FG-4400F	is released on build 5868.
FG-4401F	is released on build 5868.

Special notices

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

System Advanced menu removal (combined with System Settings)

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

PCI passthrough ports

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

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

FortiOS 6.4.0 has resolved bug 570575 to fix a FortiGate failing to provide power to ports. The PoE hardware controller, however, may require an update that must be performed using the CLI. Upon successful execution of this command, the PoE hardware controller firmware is updated to the latest version 2.18:

```
diagnose poe upgrade-firmware
```

AWS-On-Demand image

Bug ID	Description
589605	Starting from FortiOS 6.4.0, the FG-VM64-AWSONDEMAND image is no longer provided. Both AWS PAYG and AWS BYOL models will share the same FG-VM64-AWS image for upgrading and new deployments. Remember to back up your configuration before upgrading.

Azure-On-Demand image

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

FortiClient EMS Cloud registration

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

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

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

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

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

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.

Part numbers of supported FG-10xF Generation 2 models

The following part numbers are Generation 2 models that are supported in FortiOS 6.4.6 on build 6131:

- FG-100F-Gen2 P24589-20
- FG-101F-Gen2 P24605-20

Changes in CLI

Bug ID	Description

672183	Disable IHP IPsec anti-replay, and also use large MTU check values in NAT traversal sessions to avoid fragmentation and MTU exceptions. This affects the FG-3800D.
	`config system npu`
	`    set uesp-offload  {enable | disable}`
	`end`

697566	Allow ip_no_pmtu_disc to be set manually under `config system global` by adding am option to configure PMTU discovery. This value will set the kernel value for ip_no_pmtu_disc (default = 1).
	`config system global`
	`    set pmtu-discovery {enable | disable}`
	`end`

Changes in table size

Bug ID	Description
699766	Increase `system.dns-database` table size from 256 per VDOM and 512 global, to 1024 per VDOM and unlimited global.
712616	Increase `firewall.service.custom` table size from 16,384 per VDOM to 32,768 on FortiGate 3000 series models and higher.
713686	Increase `router.static6` table size from 500 per VDOM to 2000 per VDOM on FortiGate 600 series models and higher.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
634006	OpenSSL updated to 1.1.1i for security fixes.

644218	The host protection engine (HPE) has been enhanced to add monitoring and logging capabilities when the HPE is triggered. Users can enable or disable HPE monitoring, and configure intervals and multipliers for the frequency when event logs and attack logs are generated. These logs and monitors help administrators analyze the frequency of attack types and fine-tune the desired packet rates in the HPE shaper.
	`config monitoring npu-hpe`
	`  set status {enable | disable}`
	`  set interval <integer>`
	`  set multipliers <m1>, <m2>, ... <m12>`
	`end`
	The interval is set in seconds (1 - 60, default = 1). The multiplies are twelve integers ranging from 1 - 255, the default is `4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, 8`.
	An event log is generated after every (interval × multiplier) seconds for any HPE type when drops occur for that HPE type. An attack log is generated after every (4 × multiplier) number of continuous event logs.

670345	Support Strict-Transport-Security in HTTPS redirect.

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`

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 a 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.

Bug ID	Description

679245	This enhancement allows a FortiGate to use the WISPr-Bandwidth-Max-Down and WISPr-Bandwidth-Max-Up dynamic RADIUS VSAs (vendor-specific attributes) to control the traffic rates permitted for a certain device. The FortiGate can apply different traffic shaping to different users who authenticate with RADIUS based on the returned RADIUS VSA values. When the same user logs in from an additional device, the RADIUS server will send a CoA (change of authorization) message to update the bandwidth values to 1/*N* of the total values, where *N* is the number of logged in devices from the same user.
	`config firewall policy`
	`  edit 1`
	`  set dynamic-shaping {enable | disable}`
	`  next`
	`end`

681600	Add support for syslog RFC 5424 format, which can be enabled when the syslog mode is UDP or reliable.
	`config log syslogd setting`
	`  set format {default | csv | cef | RFC5424}`
	`end`

690179	The SD-WAN REST API for health-check and sla-log now exposes ADVPN shortcut information in its result. The `child_intfs` attribute returns the statistics for the corresponding shortcuts. The following command displays real-time SLA information for ADVPN shortcuts: `# diagnose sys sdwan sla-log <health check name> <sequence number> <child name>`
690711	Synchronize wildcard FQDN IPs to other autoscale members whenever a peer learns of a wildcard FQDN address.
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
694102	Improve the session in/out dev handling when the session is dirty, re-routing occurs, and so on. Avoid clearing the session in/out dev, and only update it when is changes.

700073	Add a default-action into `youtube-channel-filter configuration` to apply a default action to all channels when there is no match.
	`config videofilter youtube-channel-filter`
	`  edit <id>`
	`  set default-action {block | monitor | allow}`
	`  set log {enable | disable}`
	`  next`
	`end`
	The default settings are `monitor` for `default-action`, and `disable` for `log`.

Bug ID	Description
704819	Using the RADIUS attribute Tunnel-Private-Group-Id, a wireless controller can now accept a VLAN name as a string, and match the VLAN sub-interface attached to a VAP interface when dynamically assigning a VLAN. Users logging into an SSID can be dynamically assigned to the proper VLAN based on the VLAN configurations on RADIUS for the particular user.
711577	Add warnings to inform users when an installed firmware is not signed by Fortinet. The warning message appears in the CLI when the uploaded firmware fails signature validation, and when logging in to the FortiGate from the GUI. Additional messages are added in various places once a user is logged in to the GUI to remind them of the unsigned firmware.

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

- FortiAnalyzer 6.4.6
- FortiManager 6.4.6
- FortiClient EMS 6.4.3 build 1600 or later
- FortiClient 6.4.3 build 1608 or later
- FortiAP 6.4.4 build 0456 or later
- FortiSwitch 6.4.5 build 0461 or later

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

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

13. FortiWLC
14. FortiNAC
15. FortiVoice

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.6. When Security Fabric is enabled in FortiOS 6.4.6, all FortiGate devices must be running FortiOS 6.4.6.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.6 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 6.4.6 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 6.4.6 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 6.4.6 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 6.4.6, 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 6.4.6.

To configure `local-access` profile:

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

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

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

FortiGate VM with V-license

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

To enable `split-vdom`:

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

FortiGate VM firmware

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

Citrix Hypervisor 8.1 Express Edition

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V Server 2019 and Windows Server 2012R2 with Hyper-V role

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

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

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

WanOpt configuration changes in 6.4.0

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

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

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

```
    next
end
```

WanOpt and web cache statistics

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

IPsec interface MTU value

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

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

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

HA role wording changes

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

Virtual WAN link member lost

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

Enabling match-vip in firewall policies

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

Product integration and support

The following table lists FortiOS 6.4.6 product integration and support information:

Web Browsers	• Microsoft Edge 90 • Mozilla Firefox version 88 • Google Chrome version 90 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 19. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 6.4.6 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 19. 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 19 and Fortinet Security Fabric upgrade on page 19. 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 0297 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	• 3.2.1
AV Engine	• 6.00162
IPS Engine	• 6.00091
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 88 Google Chrome version 90
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 88 Google Chrome version 90
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 88 Google Chrome version 90
macOS Big Sur 11.0	Apple Safari version 14 Mozilla Firefox version 88 Google Chrome version 90
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 6.4.6. For inquires about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
650160	When using email filter profile, emails are being queued due to IMAP proxy being in stuck state.

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.
683835	Files fail to open in some CIFS setups where FortiOS cannot generate a signature.
707186	Scanunit crashes with signal 11 when users attach files in the Outlook Web App.

Application Control

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

DNS Filter

Bug ID	Description
682060	DNS proxy is holding 60% memory caused by retransmitted DNS messages sent from DNS clients, which causes the FortiGate to enter conserve mode.
693551	DNS filter is not working on active VDOM in second HA unit in virtual cluster environment.

Endpoint Control

Bug ID	Description
691477	EMS dynamic address synchronization delay in FortiGate IPv4 policy.

Explicit Proxy

Bug ID	Description
654455	Proxy policy destination address set to none allows all traffic.
681054	Web proxy users are disconnected due to external resource update flushing the user even if they do not have an authentication rule using the related proxy address or IP list.
689002	Proxy traffic failed after modifying resource setting in external connector.
697566	Explicit proxy unable to access a particular URL (https://***.my.salesforce.com) after upgrading from 5.6.12 to 6.2.7.
700451	Wrong source IP used intermittently when FortiGate has SD-WAN and is transparently proxy forwarding to explicit proxy.

Firewall

Bug ID	Description
474612	SNAT is using low ports below 1023 for NTP.
595949	Any changes to the security policy table causes the hit count to reset.
644225	Challenge ACK is being dropped.
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed.
683426	No hit counts on policy for DHCP broadcast packets in transparent mode.
683669	Firewall schedule settings are not following daylight saving time.
694154	Dynamic traffic shapers are not consistent in their idle time limit.
696619	FGSP synchronized UDP sessions may be blocked in NGFW policy mode when asymmetric routing is used due to a policy matching failure. Other types of traffic may also be affected (such as TCP) in the case of failover of the reply direction traffic to a different FortiGate in the FGSP cluster.
699785	Firewall performance may degrade when thousands of VIPs are configured.

FortiView

Bug ID	Description
621453	FortiGate cannot get detailed information on FortiClient vulnerabilities from FortiAnalyzer.
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.
683413	Some FortiView pages/widgets fail to query data from FortiAnalyzer Cloud if the local FortiAnalyzer is not enabled. 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.
592854	An address created by the VPN wizard cannot save changes due to an incorrect validation check for parentheses, *()*, in the *Comments* field.
599815	Add support for case-insensitive inspecting the username of an email address.
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.
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*.
647431	After removing an image name on the *Replacement Messages Edit* page, an image list should be displayed when hovering the mouse over the image URL link, but it is not.
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.
656599	After upgrading firmware, the CLI script action has a required administrator profile to restrict capabilities. This profile cannot exceed the current administrator's permissions. When configuring a stitch, an administrator can only choose a CLI script that has equal or lesser permissions that the current administrator.
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.

Bug ID	Description
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.
665597	When `set server-identity-check` is enabled, *Test User Credentials* fails when performed on the CLI and passes when run from the GUI. The GUI implementation has been updated to match that of the CLI.
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*.
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.
674548	When searching for a *Firewall Policy*, if the search keyword is found in the policy name and there are spaces adjacent to it, the search results will be displayed without the adjacent spaces. The actual policy name is not changed.
674592	When `config ha-mgmt-interfaces` is configured, the GUI incorrectly shows an error when setting overlapping IP address.
680804	On the *SD-WAN Rules* page, the default implicit rule shows a destination address of *Route tag: undefined*.
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.
682547	Unable to change *System Settings* when in split VDOM mode; the error *Administration settings failed to save* is displayed.
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.

Bug ID	Description
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.
697667	When the FortiGate is managed by FortiManager, an administrator that selects *Login Read-Only* is incorrectly allowed to select *Update firmware* in *System* > *Firmware*, browse for an image, and install it.
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.
703955	When editing the WAF profile in the GUI, changes to the WAF `default-allowed-methods` are not committed. The CLI must be used.
704209	When updating the *Disclaimer Page* replacement message, if the message is too long, the *Save* button is disabled and a red warning displays the current buffer size compared to the allowed size.
704638	Add column for *Absolute Date/Time* to the GUI *Log Viewer*.
706711	When `accprofile` is set to `fwgrp custom` with all read-write permissions, some GUI menus will not be visible. Affected menu items include *IP Pools*, *Protocol Options*, *Traffic Shapers*, and *Traffic Shaping Policy/Profile*.
710946	Special characters not allowed in the OU field of a CSR signing request, from both the GUI and CLI.
713580	Non-FortiToken RADIUS two-factor authentication not working when logging into the GUI.
715256	When the *Security Fabric Connection* is enabled on a VPN interface, the *DHCP Server* section disappears from the GUI.

HA

Bug ID	Description
659837	The HA secondary cannot synchronize a new virtual switch configuration from the primary.
670331	Management access not working in transparent mode cluster after upgrade.
671288	FortiGate in standalone mode has a virtual MAC address.
684051	IPv6 link local address is not generated in FGCP.
690248	Malicious certificate database is not getting updated on the secondary unit.
692212	The interfaces on NP6 platforms are down when doing a configuration revert in HA mode.
693178	Sessions timeout after traffic failover goes back and forth on a transparent FGSP cluster.
693223	hasync crashes with signal 11 in `ha_same_fosver_with_manage_master`.
714113	GRE configuration should not be synchronized in multi-AZ HA, but the system does not allow it to be added in the VDOM exception.

Intrusion Prevention

Bug ID	Description
686301	ipshelper CPU spikes when configuration changes are made.
688888	BZIP2 file including EICAR is detected in the original direction of the flow mode firewall policy even though `scan-bzip2` is disabled.
689259	Flow-Based AV scanning does not send specific extension files to FortiSandbox.
691395	Signature false positives causing outage after IPS database update.
694777	Application, IPS, and AV databases and engines are not updated by scheduled updates if a security policy is used.

IPsec VPN

Bug ID	Description
578879, 676728	IPsec tunnel bandwidth usage is not correct on the GUI widget and SNMP graph when NPU is doing host offloading.
658215	When the SA is about to expire, before it is removed it is not offloaded so the traffic may not go through.
659442	NP6Lite platforms may enter conserve mode because the `get/put` reference count for `pinfo` is not reasonable. When there is an inbound SA update, the old `pinfo` is not freed.
690903	ADVPN shortcut is flapping when spokes are behind one-to-one NAT.
691878	Creating or updating a user with two-factor authentication causes dialup VPN traffic to stop.
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.
694992	Issue establishing IPsec and L2TP tunnel with Chromebook behind NAT.
709850	Duplicate IP assigned by IKE Mode Config due to static gateway being out of sync after HA flapping. The tunnel that is out of sync cannot receive the deletion from the hub and holds on to an IP that has already been released.
710961	Hub is dropping packets due to `Failed to find IPsec Common` after upgrading from 6.2.6 to 6.2.7.

Log & Report

Bug ID	Description
661040	Cyrillic characters not displayed properly in local reports.
677540	First TCP connection to syslog server is not stable.
682444	No event log generated when log disk needs format.
696825	In rare cases, reportd crashes when the number of items can be zero, but the pie chart is still generated successfully.
710344	Reliable syslog is sent in the wrong format when flushing the logs queued in the log daemon when working in TCP reliable mode.
711946	FortiAnalyzer cannot process the packet loss field in the log because the field has a `%` in it.

Proxy

Bug ID	Description
634117	WAD crash on reconnect bypass. With a special timing, when the server triggers error handling that results in the WAD bypassing the SSL connection, the server-side TCP port is already closed, and the `wad_sched_event` object is already freed.
670339	Proxy-based SSL out-band-probe session has local out connection. Since the local out session will not learn the router policy, it makes all outbound connections fail if there is no static router to the destination.
682980	Proxy deep inspection workaround needed for sites that require psk_key_exchange_modes.
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.
691468	WAD IPS crashes because task is scheduled after closing.
692462	Transparent proxy implicit deny policy is not blocking access.
693441	WAD crashes at `wad_client_cert_req_act_get` when SSL layer configuration is cleaned up after policy matching.
693951	Cannot access Java-based application in proxy mode.
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.
700073, 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.

REST API

Bug ID	Description
597707	REST API `/api/v2/monitor/firewall/security-policy` adds UUID data for security policy statistics.
663441	REST API unable to change status of interface when VDOMs are enabled.
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.
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
579884	VRF configuration in WWAN interface has no effect after reboot.
684378	Traffic is forwarded out to the wrong interface if an LTE interface is an SD-WAN member. The LTE interface may lose its SD-WAN flag during modem initialization.
685871	OSPFv3 routes are missing from routing table when unsetting or setting the ASBR table.
686829	ADVPN and SD-WAN reply direction randomly chooses ECMP path rather than following shortcut.
690164	FortiGuard DDNS does not follow FortiGuard interface select method, and it does not support HA failover functionality.
691687	Return packets are not always sent back through the correct path.
692241	BGP daemon consumes high CPU in ADVPN setup when disconnecting after socket writing error.
693238	OSPF neighbor cannot form with spoke in ADVPN setup if the interface has a parent link and it is a tunnel.
693496	SD-WAN rules not working for FortiAnalyzer settings because the `interface-select-method` is implemented on a remote device FortiAnalyzer/FDS but not added to FortiView/log viewing API.
697658	FortiCloud activation does not honor the `set interface-select-method` command under `config system fortiguard`.
698360	OSPF area range routes lost during HA failover.
700537	GRE configuration fails on MAP-E interface (vne.root).
703782	Traffic to FortiToken Mobile push server does not follow SD-WAN/PBR rules.

Bug ID	Description
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.
705767	SD-WAN rules are not working with route tags and VRF.
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
650724	Invalid license data supplied by FortiGuard/FortiCare causes invalid warning in the *Security Rating* report.

SSL VPN

Bug ID	Description
586035	The policy `script-src 'self'` will block the SSL VPN proxy URL.
610995	SSL VPN web mode gets error when accessing internal website at https://st***.st***.ca/.
659322	SSL VPN disconnects all connections after adding new address to IP pool.
669506	SSL VPN web mode cannot load web page https://jira.ca.ob***.com properly based on Jira application.
669663	There are potential cases where the UDP redirect port is used by other parts of the system, which causes SSL VPN to restart.
670731	Internal application server/website bookmark (https://***.***.***.***:****/nexgen/) not working in SSL VPN web mode.
672743	sslvpnd segmentation fault crash due to old DNS entries in cache that cannot be released if the same results were added into the cache but in a different order.
675204	JSON parse error returned SSL VPN web mode for website https://bi***.u***.cat/az.php.
677031	SSL VPN web mode does not rewrite playback URLs on the internal FileMaker WebDirect portal.
678996	Customized replacement messages for SSL VPN login page sometimes cannot be parsed correctly, causing the FortiToken authentication page to not appear.
680744	Internal SolarWinds Orion platform's webpages have issue in SSL VPN web mode.

Bug ID	Description
681424	Unable to access sc***.com in SSL VPN web mode.
681764	Video could not load for https://le***.sm***.ca in SSL VPN web mode.
683601	Changing DNS or WINS server under VPN SSL settings logs off connected users.
683963	SSL VPN bookmark fails to authenticate user through single sign-on for internal website login.
684012	SSL VPN crashed with signal 11 (segmentation fault) `uri_search` because of rules set for a special case.
684866	Specific content in portal.ag***.com cannot be shown in SSL VPN web mode.
688023	SSL VPN bookmarked website shows empty page after logging in to SSL VPN gateway https://vd***.vi***.com.
689616	When a client is connected to SSL VPN and has an internet outage for more then 15 seconds, the client fails to reconnect.
690217	Unable to display the data in SSL VPN web mode on innovaphone PBX link.
690282	Access through web portal to an Opengear Lighthouse server does not load the login page properly.
690507	SSO login for the bookmark to access FortiAnalyzer GUI does not work.
690686	Certificate authentication does not check PKI users in the expected order.
694226	SSL VPN web mode removes ant-tree components in HTML source.
696009	Tunnel IP pool leak when DTLS tunnel user session is deleted due to timeout (idle or authentication).
700673	Unexpected group to portal matching priority with SAML authentication.
703007	SSL VPN web mode has problem accessing https://mf***.sa***.com.sa/Login.aspx?url=Default.aspx.
705695	OS check for SSL VPN tunnel is not working on macOS Big Sur; the connection is rejected when the action is set to allow.
706185	OWA user details are not showing in SSL VPN web mode.
706270	sslvpnd `signal 11 (Segmentation fault) received` caused by a pointer arithmetic error.
710163	SSL VPN stuck loading https://el***.***-data.pl when wrong credential was entered.
714604	SSL VPN daemon may crash when connection releases.

Switch Controller

Bug ID	Description
690904	Unable to de-authorize FortiSwitch, or assign VLAN on FortiSwitch port on a tenant VDOM.

Bug ID	Description
691985	L3 managed FortiSwitch configuration synchronization error due to the empty string parameter in `ptp-policy` on managed port configuration.
696405	`disable-discovery` of a FortiSwitch on one VDOM should not make the FortiSwitch disconnect from another VDOM.
700220	A limit is needed to prevent changes to `default-virtual-switch-vlan` in the tenant VDOM if there already are leased FortiSwitch ports.
700310	When managed switch PTP policy and settings configuration was pushed as part of initial FortiLink configuration, the FortiLink connection is in an error state.
700842	FortiSwitch MAC delete logs are not being generated.
702942	FortiLink trunk is not formed on FortiSwitch connecting to FortiGate. When managed switches are learned on the software switch and hardware switch, they were deleted from the CLI, and `fortilinkd` did not clear the states for those switches so new switches were not learned.

System

Bug ID	Description
568399	FG-200E has `np6lite_lacp_lifc` error message when booting up a device if there are more than seven groups of LAGs configured.
572038	VPN throughput dropped when FEC is enabled.
616576	DoS log counters are inaccurate (policy counters, event log entries, packet counts).
648406	Flow-based inspection with virtual wire pair causes MAC to flap.
650411	SSL local certificate can not be imported via CMDB API (`api/v2/cmdb/vpn.certificate/local`) due to certificate data handling in CMF plugin (`vpn.certificate/local`).
655555	Unable to sniff LLDP frames on management and TFTP ports.
660441	When a PPPoE interface is enabled, it overwrites the LAN address object that was created.
663826	Fortinet Factory certificate key integrity check failed in `diagnose hardware certificate` command.
664279	snmpd crashes when sorting a list-based ARP table if it has about 50,000 or more entries.
666210	`diagnose sys csum` command shows wrong hash on SOC4 appliances (FG- 60F, FG-61F, FG-100F and FG-101F).
666418	SFP interfaces on FG-330xE do not show link light.
667307	Console prints out `NP6XLITE: np6xlite_hw_ipl_rw_mem_channel timeout` message on SoC4 platforms.

Bug ID	Description
668856	Offloaded traffic passing through two VDOMs connected with EMAC-VLANs is sometimes dropped.
671972	If `cfg-save` is set to manual (under `config system global`), it causes problems with the queries made when parsing the internet service database.
672065	CMDB may crash during boot up when querying VPN SSL settings.
672183	UDP 4500 inter-VDOM traffic is not offloaded, causing BFD/IPsec to drop.
675842	Get `Failed on update FortiGuardDDNS` error for fortiddns when secondary device becomes primary device in an HA cluster.
677263	When changing the interface speed, some checking is skipped if it is set from FortiManager.
677568	Failed to parse `execute restore config` properly when the command is from a FortiManager script.
678469	Configuration attribute field in system event logs has length limitation.
678734	GeoIP6 address causes policy to not install properly in the kernel.
680881	Rebooting device causes interface mode to change from static to DHCP.
681478	After reboot, `get global.system.interface.npu0_vlink0 config` error when VDOM is in transparent mode.
686442	Traffic was stopped because PBA IP pool has the wrong relationship information.
686539	Egress interface-based traffic shaping is not applied if the session is processed by NTurbo.
687519	Bulk changes through the CLI are very slow with 24000 existing policies.
688316	After upgrading from 6.4.2 to 6.4.4, some configurations moved to another VDOM.
689317, 698927	After pushing the interface configuration from FortiManager, the device index is incorrectly set to 0.
689873	Sometimes a VWL service adds a child without a parent, leading to a `signal 6 (Aborted)` crash received at `cmf_query_ses_update_child`.
690762	Application lted signal 11 crash on FWF-40F-3G4G.
690797	Huawei E8372h-320 LTE modem does not receive IP on FG-30E.
691858	The newcli process crashes or shows an error when creating a VIP with the same external interface IP but a different source address filter.
692490	When an `<entry name>` is on the same line as `config <setting> <setting> <entry name>`, it is not handled properly to send to FortiManager.
693757	Secondary FG-5001D blades in SLBC cluster do not show updated contract dates.
694754	Cloning a firewall policy may cause cmdbsvr to crash.
696517	NPU6 is not able to support WCCP traffic offloading. NTurbo driver received packet, which included additional IPv4 header and WCCP header. NTurbo is unable to process this kind of packets so it dropped.

Bug ID	Description
696622	FortiGate cannot get gateway from built-in LTE modem on all LTE capable FortiGate platforms.
698005	In some environments, host-side DPDK affects the benchmark result.
698014	When running `execute speed-test` command, it shows all VLAN and SSL interfaces from other VDOMs.
700513	802.1x wiredap does not correctly process the TagID in the Tunnel-Private-Group-ID attribute.
706131	When processing visibility log requests and passively learning FQDNs and wildcard FQDN addresses at a high rate, the CPU usage of dnsproxy can reach 90% or higher.
710807	FGR-60F WAN1 and WAN2 fail to connect to the network due to board ID GPIO assignment being incorrect.
710934	FortiGate loses its DHCP lease, which is caused by the DHCP client interface turning into initial state (from that point dhcpcd will send out discover packets), but old IPs and router are still in the kernel, so it can reply to the ICMP request. That causes the customer's DHCP server (a router) to fail to assign the only available IP in the pool.
715054	Add downgrade code for DHCP server so it can be used in DHCP relay.
735492	Many processes are in a "D" state due to `unregister_netdevice`.

User & Authentication

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW.
658228	The authd and foauthd processes may crash due to crypto functions being set twice.
662404	Wildcard LDAP users created on FortiToken Cloud have the first character of the username removed.
688973	OCSP verification fails with `Can't convert OCSP rsp` error after upgrading.
697278	SAML entity ID can only be entered in HTTP format, but as per standard should also support URN.
707578	If a certificate authentication job expires in fnbamd, an error is returned to caller that makes the proxy block client traffic.
712354	Firewall policy does not allow multiple SAML users that reference the same SAML server.

VM

Bug ID	Description
689239	Azure route table is not using the proper subscription ID during failover.

Bug ID	Description
690863	EIP iAzure route table is not using the proper subscription ID during failovers not updating properly with `execute update-eip` command in Azure with standard SKU public IP in some Canadian regions, like CanadaCentral and CanadaEast.
695957	Azure SDN connector gets an empty IP list when the REST API call fails, which results in IPsec connection being interrupted until the next SDN connector update succeeds (one-minute interval).
698810	Bootstrap does not work with FG-VM on Azure Stack.
700381	FG-VM kernel panicked and reboot after sending through IPv6 traffic.
713279	After rebooting a GCP FortiGate, it takes more than 30 to 40 minutes to come up and affects passthrough traffic during this period.

WAN Optimization

Bug ID	Description
686729	Transparent mode configuration was not learned properly in 6.4.

Web Application Firewall

Bug ID	Description
624452	`user-agent` setting under `config system external-resource` does not accept XSS characters.

Web Filter

Bug ID	Description
593203	Cannot enter a name for the web rating override or save it due to name input error.
668325	A hanging FortiGuard connection is not torn down in some situations.

WiFi Controller

Bug ID	Description
529727	The configured MAC address of the VAP interface did not take effect after rebooting.
621346	Dynamic VLAN on SSID cannot pass traffic through FG-100F/101F and FG-60F/61F when offloading is enabled.
686631	Wireless country setting option needs to remove sanctioned countries and add missing countries.
690483	Wireless default WTP profile not synchronized between FWF-61E with HA A-A mode.
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.
699187	SSH session shows periodical `cw_ac_wl_cfg_2_dinfo`.
699905	FAP-421E does not come online over IPsec tunnel and shows a certificate error.
707635	AP with MAC E0-23-FF not coming online through mesh with FortiWiFi radio set to root.
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.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
677844	FortiOS 6.4.6 is no longer vulnerable to the following CVE Reference: • CVE-2021-26092

Known issues

The following issues have been identified in version 6.4.6. For inquires about a particular bug or to 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.

Application Control

Bug ID	Description
701926	Stress test with application control only results in packet drops.

Endpoint Control

Bug ID	Description
685549	Need to check EMSC entitlement periodically inside fcnacd.
687320	When using FortiClient EMS, renaming the imported CA results in an authentication error. This error does not occur if the CA is not renamed.

Explicit Proxy

Bug ID	Description
733863	Get 504 gateway timeout error when trying to access proxy.pac from remote users using dialup IPsec VPN.

Firewall

Bug ID	Description
694284	In transparent mode when HA is enabled, if the packet passes through the FortiGate more than once time, the MAC address could be different from main session.
707854	FortiGate is not able to resolve FQDNs without DNS suffix for firewall address objects.
709832	When there are multiple internet services configured that match a certain IP, port, or protocol, it may cause the wrong policy to be matched.
714198	When in transparent mode with AV and IPS, the original and reply direction traffic should be redirected only one time.
714647	Proxy-based policy with AV and web filter profile will cause VIP hairpin to work abnormally.
716317	IPS user quarantine ban event is marking the sessions as dirty.
719925	Load balancing is not allowed with a flow-based policy, even if the server type is configured as IP or TCP.

FortiView

Bug ID	Description
683654	FortiView pages with FortiAnalyzer source incorrectly display a *Failed to retrieve data* error on all VDOM views when there is a newly created VDOM that is not yet registered to FortiAnalyzer. The error should only show on the new VDOM view.
722543	The *Used Quota* cannot be sorted on the *FortiGuard Quota Monitor*. The *Used Quota* column has now been split into two sortable columns: *Used Traffic Quota* and *Used Time Quota*.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
589231	When using the GUI to edit an *IP/Wildcard Mask* that was created using the CLI, the error message *Invalid IP/Wildcard mask.* is displayed.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.

Bug ID	Description
653952	*The web page cannot be found* is displayed when a dashboard ID no longer exists. **Workaround**: load another page in the navigation pane. Once loaded, load the original dashboard page (that displayed the error) again.
688016	GUI interface bandwidth widget does not show correct data for tunnel interface when ASIC offload is enabled on the firewall policy.
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI *Forward Traffic* log page can take time to load if there is no specific filter for the time range. **Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs.
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.
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 FortiAnalyzer is configured, the HTTPS daemon may crash when processing some FortiAnalyzer log requests. There is no apparent impact on the GUI operation.
719694	When there is a connection issue between the FortiGate and a managed FortiSwitch, httpsd may crash when navigating between *Switch Controller* related GUI pages.
721710	Data fails to load when the Security Fabric is enabled for a downstream FortiGate that has an upstream PPPoE interface to connect to the root.
722832	When LDAP server settings involve FQDN, LDAPS, and an enabled server identity check, the following LDAP related GUI items do not work: LDAP setting dialog, LDAP credentials test, and LDAP browser.
724394	When a RADIUS server address is defined as an FQDN, GUI tests for connectivity and user credentials fail.
727035	Unable to change FortiSwitch port status when native VLAN is empty.
727644	When the first row of sequence group in a policy table is deleted, the sequence group disappears.
735248	On a mobile phone, the WiFi captive portal may take longer to load when the default firewall authentication login template is used and the user authentication type is set to HTTP. **Workaround**: edit the login template to disable HTTP authentication or remove the href link to googleapis.
739543	On the *Network* > *Interfaces* page, unable to create or edit a VLAN switch as the VLAN ID validation incorrectly fails. **Workaround**: use the CLI.
743477	On the *Log & Report* > *Forward Traffic* page, filtering by the *Source* or *Destination* column with negation on the IP range does not work.

Bug ID	Description
745325	When creating a new (public or private) SDN connector, users are unable to specify an *Update interval* that contains *60*, as it will automatically switch to *Use Default*.
745998	An IPsec phase 1 interface with a name that contains a `/` cannot be deleted from the GUI. The CLI must be used.

HA

Bug ID	Description
669301	When sending UDP packets, hasync code uses the wrong buffer size so that it may overwrite beyond the buffer to other corrupted memory.
678145	GUI shows a warning icon that the cluster is out of sync although the cluster is in sync.
692384	High memory usage of hasync process on FGCP passive device.
695067	When there are more than two members in a HA cluster and the HA interface is used for the heartbeat interface, some RX packet drops are observed on the HA interface. However, no apparent impact is observed on the cluster operation. **Workaround**: do not use the HA interface as a heartbeat interface.
697066	When SLBC HA has a fast flip, there is a chance that the route will be deleted from the secondary when it changes to the primary.
703047	`hbdev` goes up and down quickly, then the cluster keeps changing rapidly. `hasync` objects might access invalid cluster information that causes it to crash.
703719	`hasync` is busy when receiving ARP when there is a huge number of ARPs in the network.
708928	The `set override disable` setting changes to enabled on main virtual cluster after rebooting (flag of second virtual cluster remains disabled).
710236	Heartbeat interfaces do not get updated under `diagnose sys ha dump-by <group |memory>` after HA `hbdev` configuration changes.
721720	Performance degradation of session synchronization after upgrading.
722284	When there is a large number of VLAN interfaces (around 600), the FortiGate reports `VLAN heartbeat lost on subinterface vlan` error for multiple VLANs.
723130	`diagnose sys ha reset-uptime` on the secondary devices triggers a failover on a cluster with more than two members.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.
680501	Destination interfaces are set to unknown for previous ADVPN shortcuts sessions.
721462	Memory usage increases up to conserve mode after upgrading IPS engine to 5.00239.

IPsec VPN

Bug ID	Description
699834	ESP errors are logged with incorrect SPI value.

Log & Report

Bug ID	Description
726900	No traffic logs are shown after an overnight run.

Proxy

Bug ID	Description
520176	Multiple WAD crashes observed with signal 6. The issue could be reproduced with a slow server that will not respond the connection in 10 seconds, and if the configuration changes during the 10 seconds.
604681	WAD process with SoC SSL acceleration enabled consumes more memory usage over time, which may lead to conserve mode. **Workaround**: disable SoC SSL acceleration under the firewall SSL settings.
615391	Reusing the buffer region causes frequent WAD crashes.
690387	wad_proto_stats crashes a few times.

Bug ID	Description
692444	WAD memory leak is caused by missing a close event. The WAD receives a close event from TCP when the SSL port is blocked by the up application layer. If the SSL port input buffer does not have any data, then the close event will get ignored even if the application layer turns off blocking and the SSL port will leak.
712584	WAD memory leak causes device to go into conserve mode.
714610	Explicit proxy policy (ISDB and IP pool) cannot be set in the GUI or CLI.
716400	Certificate inspection is not working as expected when an external proxy is used.
719681	Flow control failure occurred while transferring large files when `stream-scan` was running, which sometimes resulted in WAD memory spike.
722481	Proxy-based inspection causes browser to show *ERR_CONNECTION_CLOSED* message.
725628	WAD HTTP parser string leak for hostname and scheme with `trace-auth-no-rsp` enabled.
727349	Traffic is stuck if HTTP POST does not have an end of boundary.
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.

Routing

Bug ID	Description
661270	OSPF is stuck in loading state when there is a large amount of OSPF interfaces.
683742	DNS local out traffic cannot match SD-WAN rule when its member is not in VRF 0.
693396	hasync daemon was busy in dead loop if FD resource was used up when flushing routes from the kernel.
706237	ICMP *Destination Host Unreachable* responses are sent in reverse order.
712586	SNAT sessions on the original preferred SD-WAN member will be flushed after the preferred SD-WAN member changes, so existing SNAT traffic will be interrupted.
730208	Traffic is not going through when the returning interface is changed.

Security Fabric

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

Bug ID	Description
687238	FortiManager cannot install a policy due to conflict with certificate synchronization from the Security Fabric.
718581	If HA management interface is configured, the Kubernetes connector fails to connect.

SSL VPN

Bug ID	Description
550819	guacd is consuming too much memory and CPU resources during operation.
662615	FG-80F series should support a total of 96 WTP entries (48 normal).
677548	In SSL VPN web mode, options pages are not shown after clicking the option tag on the left side of the webpage on an OWA server.
677668	sslvpnd crashes due to wrong application index referencing the wrong shared memory when daemons are busy. Crash found when RADIUS user uses Framed-IP.
686425	When accessing an application in SSL VPN web mode (Sage HR), images fail to load for http://S-***.ro***.de/mp***/.
687433	Webpage is not loading via SSL VPN web mode bookmark.
689901	SharePoint links (su***.com) not working properly on webpage launched by SSL VPN web portal.
693347	Forward traffic for SSL VPN with EMS tags dynamic address is failing apart from helper-based traffic.
693691	VPN logs do not show any bandwidth utilization in SSL web tunnel statistics when only using RDP.
695404	WALLIX personal bookmark issue in SSL VPN portal.
695763	FortiClient iOS 6.4.5 has new feature that allows bypassing of 2FA for SSL VPN 2FA. The FortiGate should allow access when 2FA is skipped on FortiClient.
699587	SSL VPN policy matching problem when a local user has the same name as a pure remote user.
699619	SSL VPN web mode fails to access to https://www.we***.org.
702493	CMS URLs incorrectly rewritten by SSL VPN proxy in web mode.
715928	SSL VPN signal 11 crashes at `sslvpn_ppp_associate_fd_to_ipaddr`. For RADIUS users with Framed-IP using tunnel mode, the first user logs in successfully, then a second user with the same user name logs in and kicks the first user out. SSL VPN starts a five-second timer to wait for the first user resource to clean up. However, before the timer times out, the PPP tunnel setup fails and the PPP context is released. When the five-second timer times out, SSL VPN still tries to use the PPP context that has already been released and causes the crash.
717193	Website cannot be accessed in SSL VPN web mode.

Bug ID	Description
718133	In some conditions, the web mode JavaScript parser will encounter an infinite loop that will cause SSL VPN crashes.
718142	The map integrated in the public site is not visible when using SSL VPN web mode.
718159	Webpage, http://10.3.24.8/ma***, is not displaying correctly in SSL VPN web mode.
720290	Internal webpage, https://172.3**.***.164/ce***/, is not loading in SSL VPN web mode.
724830	FortiGate sends authentication request to all RADIUS servers instead of only those in the default realm.
726641	Unable to load pi***.vi***-ga***.org in SSL VPN web mode.
736822	Non-US keyboard layout in RDP session with SSL VPN web mode does not work correctly.

Switch Controller

Bug ID	Description
682430	Entry created in NTP under interface configuration after failing to enable FortiLink interface.
717506	Unable to add description on shared FortiSwitch port.

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.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
627734	Optimize interface dialog and configuration view for `/api/v2/monitor/system/available-interfaces` (phase 1).
648085	Link status on peer device is not down when the admin port is down on the FortiGate.
674616	VDOM list is slow to load in GUI when there are many VDOMs configured on FG-3000D.
681791	Install preview does not show all changes performed on the FortiGate.
687398	Multiple SFPs and FTLX8574D3BCL in multiple FG-1100E units have been flapping intermittently with various devices.
698204	SNMP query for firewall policy statistics in non-root VDOM returns a `0`.

Bug ID	Description
699358	Cannot change FEC (forward error correction) on port group 13-16.
699902	SNMP query of fgFwPolTables (1.3.6.1.4.1.123456.101.5.1.2.1) causes high CPU on a specific configuration.
700314	ARP reply sent out by FortiGate but was not received on neighbor device.
702135	cmdbsvr memory leak due to unreleased memory allocated by OpenSSL.
705734	FWF-40F has random kernel panic with 6.4.4 firmware.
705878	Local certificates could not be saved properly, which caused issues such as not being able to properly restore them with configuration files and causing certificates and keys to be mismatched.
709513	SD-WAN reports phantom packet loss.
714256	A softirq happened in an unprotected session read lock and caused a self-deadlock.
714402	FortiGate crashes after reboot (`kernel BUG at drivers/net/macvlan.c:869`).
714711	NP offloading is blocking backup traffic.
715571	`config match` command is not available in the user group configuration within the root VDOM when split-task VDOM is used.
716483	DNS proxy is case sensitive when resolving FQDN, which may cause DNS failure in cases where local DNS forwarder is configured.
717203	When user changes a configurations in the CLI, cmdbsvr sends the auto update file to FortiManager at the same time. There is a timing issue that may cause the last command not be sent to FortiManager since cmdbsvr has finished sending it, but the last command is not yet stored in the auto update file.
721733	IPv6 networks are not reachable shortly after FortiGate failover because an unsolicited neighbor advertisement is sent without a router flag.
722273	SA is freed while its timer is still pending, which leads to a kernel crash.
728647	DHCP discovery dropped on virtual wire pair when UTM is enabled.
729636	FTLC1122RDNL transceiver is showing as not certified by Fortinet on FG-3800D.
731821	MAP-E DDNS update request is not sent after booting up the device.
741944	The forticron process has a memory leak if there are duplicated entries in the external IP range file.

Upgrade

Bug ID	Description
716912	SSH access may be lost in some cases after upgrading to 6.2.8, 6.4.6, or 7.0.0.

User & Authentication

Bug ID	Description
682394	FortiGate is unable to verify the CA chain of the FSSO server if the chain is not directly rooted to FSSO endpoint.
688989	Two-factor authentication can be bypassed with some configurations.
691556	Get CLI error when setting `auto-regenerate-days` option for local certificate.
698716	RADIUS password encoding does not work.

701356	When a GUI administrator certificate, `admin-server-cert`, is provisioned via SCEP, the FortiGate does not automatically offer the newly updated certificate to HTTPS clients. FortiOS 7.0.0 and later does not have this issue.
	Workaround: manually unset `admin-server-cert` and set it back to the same certificate.
	`config system global`
	`  unset admin-server-cert`
	`end`
	`config system global`
	`  set admin-server-cert <scep_certificate>`
	`end`

707868	The authd daemon crashes due to invalid dynamic memory access when data size is over 64K.
709303	SAML `user-name` and `group-name` configuration values are limited to only 35 characters.
710212	RADIUS accounting port is occasionally missing.
725056	FSSO local poller fails after recent Microsoft Windows update (KB5003646, KB5003638, ...).

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.
687925	Hardware checksum failure encountered on Azure FG-VM.
714682	GENEVE tunnel with loopback interface is not working.

Bug ID	Description
715750	EIP information is not automatically updated after instance reboot.
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.

Web Filter

Bug ID	Description
677234	Unable to block webpages present in the external list when accessing them through the Google Translate URL.

WiFi Controller

Bug ID	Description
502080	`TARGET ASSERT` error in WiFi driver causes kernel panic.
662615	FG-80F series should support a total of 96 WTP entries (48 normal).
676689	RADIUS traffic not matching SD-WAN rule when using wpad daemon for wireless connection.
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.
680527	Clients fails to authenticate to SSID due to MPSK client limit being reached when the actual connected clients are below the limit.
685593	Spectrum analysis graphs only presents a portion of the data for monitor mode radio when *X-Axis* is *MHz*.
693973	Captive portal/disclaimer is not shown for SSIDs not belonging to the default VRF.
700356	CAPWAP daemon crashing due to IoT detection.
709824	Dynamic VLAN SSID traffic cannot pass through VDOM link when `capwap-offload` is enabled.
720674	cw_acd is crashing on FG-40F.

Built-in AV engine

Resolved engine issues

Bug ID	Description
691412	Scanunit process crashes when user accesses a specific website.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
580391	Unable to create MAC address-based policies in NGFW mode.
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed. A workaround is to clear sessions after a policy change.
662698	One-arm sniffer logging shows inaccurate SNMP application sent bytes.
672994	Web filter warning message does not contain certification chain.
676705	Custom IEC-104 application control signatures skipped after signature database update.
677834	HTTP traffic is dropped when custom proxy options are applied to a policy.
681611	IPS engine crashes (5.218 `ips_dlp_alert`).
683669	Firewall schedule settings are not following daylight saving time.
688888	BZIP2 file including EICAR is detected in the original direction of the flow mode firewall policy even though `scan-bzip2` is disabled.
691196	One-arm IPS URL filter unable to block HTTPS websites.
695441	Not getting past block/override page or warning page when doing a web filter override in flow mode.
695774	Remote category flow and proxy mode wildcard matching difference
696619	FGSP synchronized UDP sessions may be blocked in NGFW policy mode when asymmetric routing is used due to a policy matching failure. Other types of traffic may also be affected (such as TCP) in the case of failover of the reply direction traffic to a different FortiGate in the FGSP cluster.
696753	Chassis has multiple IPS crashes and UTM web filter is impacted after enabling web filter content header.
696811	`IPSA self test failed, disable IPSA! IPSA disabled: self test failed` message appears in system event logs.
696819	IPS archive timestamp is dated from 1970.
702142	File filter monitor blocks files in flow AV if there is a scan error.
707907	IPS engine (flow mode deep inspection) does not decrypt some TLS 1.3 sessions, which causes problems with application control detection.
713068	FGSP support in NGFW policy mode.
715136	High memory usage for some slab objects.

Bug ID	Description
718452	`set https-replacemsg disable` causing connection RST on URLs in URL filter list (flow-based inspection).
719007	URL filtering followed by `/*` causes rating error.
719252	IPS engine crash.
721410	Unable to open fb.watch website in flow mode using SSL deep inspection with application control.
721462	Memory usage increases up to conserve mode after upgrading IPS engine to 5.00239.
724400	Facebook.com website gives error in Firefox version 89 with flow mode and deep inspection.
724767	Hostname is garbled in event log that is detected by `HTTP.Suspicious.Headers.With.Special.Characters`.

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.