FortiOS - Release Notes

Version 6.4.7

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

August 30, 2021
FortiOS 6.4.7 Release Notes
01-647-721484-20210830

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-08-26	Initial release.
2021-08-27	Updated *Supported models*, *Resolved issues*, *Known issues*, and *Built-in AV engine*.
2021-08-30	Updated *Resolved issues* and *Known issues*.

Introduction and supported models

This guide provides release information for FortiOS 6.4.7 build 1911.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.7 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-200F, FG-201E, FG-201F, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-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 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.

Changes in CLI

Bug ID	Description

645241	Remove `prp-port-out` and `prp-port-in` settings from `system npu` and replace with the following:
	`config system npu setting prp`
	`set prp-port-in port-list`
	`set prp-port-out port-list`
	`end`

688989	Change `username-case-sensitivity` option to `username-sensitivity`. This new option includes both case sensitivity and accent sensitivity. When disabled, both case and accents are ignored when comparing names during matching:
	`config user local`
	`edit <name>`
	`set username-sensitivity {enable | disable}`
	`next`
	`end`

693347	Restrict IPv6 pools address and IPv6 split tunneling routing address to be IP mask or range type only so SSL VPN can support EMS tag dynamic addresses:
	`config vpn ssl web portal`
	`edit <name>`
	`set ipv6-pools <address>`
	`set ipv6-split-tunneling-routing-address <address>`
	`next`
	`end`

Changes in default behavior

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

Changes in table size

Bug ID	Description
662615	FG-80F series supports a total of 96 WTP entries (normal 48).

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description

477886	Allow ingress and egress ports to be configured so the PRP trailer is not stripped when PRP packets come in or go out.
	`config system npu`
	`set prp-port-in <port>`
	`set prp-port-out <port>`
	`end`

489956	Add LAG implementation so each session uses the same NP6 and XAUI for ingress and egress directions to avoid fast path congestion (this setting is disabled by default).
	`config system npu`
	`set lag-out-port-select {enable | disable}`
	`end`
	Add algorithm in NPU driver for distribution, `AGG_ALGORITHM_NPU`.

566452	Support hardware switch on FG-400E and FG-1100E models. The following commands have been removed:
	`config system virtual-switch`
	`edit <name>`
	`config port`
	`edit <name>`
	`set speed <option>`
	`set status {up | down}`
	`next`
	`end`
	`next`
	`end`
	`config system physical-switch`
	`edit <name>`
	`config port`
	`edit <name>`
	`set speed <option>`
	`set status {up | down}`
	`next`
	`end`
	`next`
	`end`

641524	Add interface selection for IPS TLS protocol active probing.

Bug ID	Description

	`config ips global`
	`  config tls-active-probe`
	`  set interface-selection-method {auto | sdwan | specify}`
	`  set interface <interface>`
	`  set vdom <VDOM>`
	`  set source-ip <IPv4 address>`
	`  set source-ip6 <IPv6 address>`
	`  end`
	`end`

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.
685910	Add SoC4 driver support for the IEEE 802.1ad, which is also known as QinQ. When the OID is used up, it is forbidden to create a new QinQ interface.
692529	Enhance MAC authentication bypass so that the MAC authentication status is recorded in authd. The MAC authentication is retired in 10 seconds and is always sent to the portal for HTTP authentication sessions.
699456	Increase the generated RSA key bits from 1024 to 2048.

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`.

717907	Add option in CLI to manage how long authenticated FSSO users on the FortiGate will remain on the list of authenticated FSSO users when a network connection to the collector agent is lost.
	`config user fsso`
	`  edit <name>`
	`  set logon-timeout <integer>`
	`  next`
	`end`
	The `logon-timeout` is measured in minutes (1 - 2880, default = 5).

720371	New ciphers have been added in FIPS ciphers mode on FortiGate VMs so that cloud instances running this mode can form IPsec tunnels with hardware models running FIPS-CC mode. Added to IPsec phase 1: • aes128-sha256 • aes128-sha384 • aes128-sha512

Bug ID	Description
	• aes256-sha256 • aes256-sha384 • aes256-sha512 Added to IPsec phase 2: • aes128-sha256 • aes128-sha384 • aes128-sha512 • aes256-sha256 • aes256-sha384 • aes256-sha512

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 6.4.7 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 6.4.7. When Security Fabric is enabled in FortiOS 6.4.7, all FortiGate devices must be running FortiOS 6.4.7.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.7 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 6.4.7 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 6.4.7 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 6.4.7 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 6.4.7, 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 6.4.7.

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 6.4.7 product integration and support information:

Web Browsers	• Microsoft Edge 90 • Mozilla Firefox version 91 • Google Chrome version 92 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 18. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 6.4.7 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 18. 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 18 and Fortinet Security Fabric upgrade on page 18. 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 0301 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	• 6.00164
IPS Engine	• 6.00100
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 91 Google Chrome version 92
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 91 Google Chrome version 92
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 91 Google Chrome version 92
macOS Big Sur 11.0	Apple Safari version 14 Mozilla Firefox version 91 Google Chrome version 92
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 6.4.7. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
702142	File filter monitor blocks files in flow AV if there is a scan error.

Application Control

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

DNS Filter

Bug ID	Description
682354	SDNS block portal IP information is not available in anycast mode.

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
716224	In web proxy with transparent policy, the web filter rating fails when there is no SNI or CID.
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.
705402	Server load-balancing on FortiGate is not working as expected when the active server is down.
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.
717802	In transparent mode, a log has an irrelevant `policyid`.

FortiView

Bug ID	Description
712580	When viewing FortiView *Sources* or *Destinations*, some usernames in the format of <DOMAIN\username> are displayed as *DOMAIN\username*. The user is displayed with a \ in the CLI.
722543	FortiView does not arrange FortiGuard quota based on highest to lowest value and vice versa.

GUI

Bug ID	Description
589231	Get *Invalid IP/Wildcard mask warning* when editing the address object in the GUI.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.
676306	httpsd has signal 6 and 11 crashes at `cmf_query_create_child` because of segfault in `/api/v2/monitor/switch-controller/managed-switch/transceivers`.
696226	Interfaces and zones open slowly.
700525	In Firefox, the *System* > *Certificates* page does not display an expiry date.
709103	Unable to edit interfaces in the GUI, and httpsd is spiking the CPU cores.
713148	httpsd process has high CPU and memory usages, causing the unit to enter conserve mode.
715493	httpsd consumes high CPU when loading a GUI page.
719620	Interface page keep loading when administrator user has `netgrp read-write` permissions only and interface contains IPsec VPN.
719694	httpsd crashes when navigating between switch controller related GUI pages.
721710	*Failed to load data* message appears after enabling the Security Fabric on the device when the upstream interface is a PPPoE interface.
722832	When LDAPS is configured with FQDN and a server identity check, all LDAP-related GUI pages do not work. The CLI and fnbamd are OK.
724394	RADIUS tests in GUI and REST API do not work if the server address is an FQDN.
727035	Changes to FortiSwitch port status fail to save in the GUI.
727644	Deleting the first policy within a grouping causes other rules in that section to be moved to the previous one (global label).

HA

Bug ID	Description
634465	When sending UDP packets, `hasync` code uses the wrong buffer size, which may overwrite beyond the buffer to other corrupted memory.
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.

Bug ID	Description
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.
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.
715939	Cluster is unstable when running interface configuration scripts. For example, when inserting many VLANs, hatalk will get a lot of `intf_vd_changed` events and recheck the MAC every time, which blocks hatalk from sending heartbeat packets for a long time so that the peer loses it.
717251	In FGSP, `session-sync-dev` statistics of `get system ha status` disappear after reboot.
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
669089	IPS profile dialog in GUI shows misleading *All Attributes in the Details* field for filter entries with a CVE value.
680501	Destination interfaces are set to unknown for previous ADVPN shortcuts sessions.
693800	IPS memory spike on device running version: 5.00229.
721462	Memory usage increases up to conserve mode after upgrading IPS engine to 5.00239.

IPsec VPN

Bug ID	Description
685287	When trying to override the MTU for the tunnel interface, it cannot be set according to the underlying interface MTU.
699834	ESP errors are logged with incorrect SPI value.
710605	Enabling FEC causes BGP neighbors to disconnect after a while.
714400	Dynamic IKEv2 IPsec VPN fails to establish after adding new phase 2 with mismatched traffic selector.
715651	iked crashed when clients from the same peer connect to two different dynamic server configurations that are using RADIUS authentication.

Log & Report

Bug ID	Description
722315	System might generate garbage administrator log events upon session timeout.
726690	Forward traffic log from disk is missing for virtual wire pair policy.

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.
615391	Reusing the buffer region causes frequent WAD crashes.
616261	WAD daemon might have signal 11 crashes when SSL starts to process an event during a handshake, and the event is not in the context of FTS.
683844	In cases when WAD fails to resolve a firewall policy for the session, WAD crashes at `wad_ssl_proxy_can_bypass()` when a missed condition check allows the session to still pass through.
690387	wad_proto_stats crashes a few times.
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.

Bug ID	Description
700073, 714109	YouTube server added new URLs (`youtubei/v1/player, youtubei/v1/navigator`) that caused proxy option to restrict YouTube access to not work.
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.

REST API

Bug ID	Description
710198	`/api/v2/monitor/system/available-interfaces` takes over one minute for a response.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
661270	OSPF is stuck in loading state when there is a large amount of routes (over 6000).
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.
715274	Enabling SD-WAN on interfaces with full BGP routes leads to device going into conserve mode.
722343	SD-WAN rule not matched with MAC address object and ISDB in policy.

Bug ID	Description
723550	Load-balance service mode and maximize bandwidth (SLA) in SD-WAN rule does not work as expected.
724250	Enabling `preserve-session-route` does not take effect in SD-WAN scenario.
730208	Traffic is not going through when the returning interface is changed.

Security Fabric

Bug ID	Description
687238	FortiManager cannot install a policy due to conflict with certificate synchronization from the Security Fabric.
695040	Unable to connect to vCenter using ESXi SDN connector with password containing certain characters.
718581	If HA management interface is configured, the Kubernetes connector fails to connect.

SSL VPN

Bug ID	Description
500664	SSL VPN RDP bookmark not working with CVE-2018-0886.
515519	guacd uses 99% CPU when SSL VPN web portal connects to RDP server.
542815	SSL VPN web portal RDP connections to RDS session hosts fails.
550819	guacd is consuming too much memory and CPU resources during operation.
586035	The policy `script-src 'self'` will block the SSL VPN proxy URL.
630068	When SSL VPN SSH times out, SSH to SES will crash when SSH is empty.
662042	The https://outlook.office365.com and https://login.microsoft.com websites cannot be accessed in the SSL VPN web portal.
676333	Unable to type accents using dead keys in RDP using Spanish keyboard layout over SSL VPN web mode in macOS.
677031	SSL VPN web mode does not rewrite playback URLs on the internal FileMaker WebDirect portal.
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.

Bug ID	Description
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.
689465	RDS redirect not working on SSL VPN web portal.
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.
693718	FortiClient SSL VPN users are unable to authenticate when zero-trust tag IP address is used as the host IP under limited access.
694346	Report section of internal web server (https://lm***.lm***.au***.vw***/ar***/) is not accessible via the SSL VPN web portal.
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.
697643	Customer webpage is not loading in SSL VPN web mode with https://nb***.al**.com.eg/SFTP.
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.
701119	SSL VPN DTLS tunnel could not be established in some cases when the tunnel link is still under negotiation. Some IP packets were sent to the client, causing the client's logic to fail.
702493	CMS URLs incorrectly rewritten by SSL VPN proxy in web mode.
704597	Search option on internal website, kp***.kd****.ca, not working while accessing via SSL VPN web mode.
714700	SSL VPN proxy error in web mode due to requests to loopback IP.
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.
716622	Due to change on samld side that increases the length of the SAML attribute name to 256, SSL VPN could not correctly parse the username from the SAML response when the username attribute has a long name.
717193	Website cannot be accessed in SSL VPN web mode.
718142	The map integrated in the public site is not visible when using SSL VPN web mode.

Bug ID	Description
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
464340	EHP drops for units with no NP service module.
495532	EHP drop improvement for units with no NP service module.
567019	CP9 VPN queue tasklet `unable to handle kernel NULL pointer dereference at 0000000000000120` and device reboots.
613947	Redundant interface cannot pick up traffic if one member is down.
627734	Optimize interface dialog and configuration view for `/api/v2/monitor/system/available-interfaces` (phase 1).
645241	LACP failed to process traffic after adding new QSFP interfaces as LACP members even when the LACP status is up.
645848	FortiOS is providing self-signed CA certificate intermittently with flow-based SSL certificate inspection.
651626	A session clash is caused by the same NAT port. It happens when many sessions are created at the same time and they get the same NAT port due to the wrong port seed value.
671332	httpsd crashed after changing VDOM for interface.
674616	VDOM list is slow to load in GUI when there are many VDOMs configured on FG-3000D.

Bug ID	Description
681791	Install preview does not show all changes performed on the FortiGate.
683387, 711698	Change WWAN interface default netmask to /32 and default distance to 1.
687457	dnsproxy process crashes with signal 11.
692943	If an updated FFDB package is found, crash may happen at `init_ffdb_map` if it is called when `ffdb_map` or `ffdb_app` is already in the process of being parsed, especially in HA.
698003	When creating a new administrator, the administrator profile's reference is visible in other administrator accounts from different VDOMs.
698204	SNMP query for firewall policy statistics in non-root VDOM returns a `0`.
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.
703131	Split-task VDOM does not update IPS/AV from `ha-direct` connected internal FortiManager.
705734	FWF-40F has random kernel panic with 6.4.4 firmware.
706686	LAG interface between FortiGate and Cisco switch flaps when adding/removing member interface.
709513	SD-WAN reports phantom packet loss.
712506	25G-capable ports do not receive any traffic. Affected platforms: FG-1100E and FG-1101E.
712905	Daylight saving time changes will not reflect for time zone 16.
713599	FG-40F-3G4G experiencing kernel panics and unexpected reboots (`Unable to handle kernel NULL pointer dereference`).
714192	`diagnose sys bcm_intf cli "2:"` and `diagnose sys bcm_intf cli "ps"` try to access a non-existent BCM switches, which leads to kernel panic.
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.
715647	In VWP with `set wildcard-vlan enable`, for some special cases the SKB `headlen` is not long enough for handling. It may cause a protective crash when doing `skb_pull`.

Bug ID	Description
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.
718322	FortiGate sends an invalid configuration to FortiManager, which causes the FortiManager policy packages to have an unknown status.
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.
722287	The `set key-outbound` and `set key-inbound` parameters are missing for GRE tunnels under `config system gre-tunnel`.
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.

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
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.
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
687925	Hardware checksum failure encountered on Azure FG-VM.
714682	GENEVE tunnel with loopback interface is not working.
715750	EIP information is not automatically updated after instance reboot.

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.
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.
697058	Unable to change AP state under rogue AP's monitor page.
700356	CAPWAP daemon crashing due to IoT detection.
709824	Dynamic VLAN SSID traffic cannot pass through VDOM link when `capwap-offload` is enabled.
710759	Automation trigger for rogue AP on wire sends email alerts for rogue AP not on wire.
717227	`get wireless-controller wtp-status` output only shows only one AP entry.
720674	cw_acd is crashing on FG-40F.

Known issues

The following issues have been identified in version 6.4.7. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
665173	Crash logs are sometimes truncated/incomplete.

FortiView

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

GUI

Bug ID	Description
610572	Guest user credentials never expire if a guest user logs in via the WiFi portal while an administrator is actively viewing the user's account via the GUI. If the administrator clicks *OK* in the user edit dialog after the guest user has logged in, the user's current login session is not subject to the configured expiration time. **Workaround**: click *Cancel* instead of *OK* to close the dialog.
688016	GUI interface bandwidth widget does not show correct data for tunnel interface when ASIC offload is enabled on the firewall policy.
696573	Firewall policy is not visible in GUI when using `set internet-service src enable`.
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	Administrator logout log does not reflect the correct timeout setting if the administrator closes the browser directly.
720613	Sometimes the event log is duplicated when downloaded from the GUI.

HA

Bug ID	Description
717788	FGSP has problem at failover when NTurbo or offloading is enabled (IPv4).

Intrusion Prevention

Bug ID	Description
638341	In some cases, IPS fails to get interface ID information that would result in IPS incorrectly dropping the session during static matching.
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.

IPsec VPN

Bug ID	Description
668997	*Duplicate entry found* error shown when assigning multiple dialup IPsec tunnels with the same secondary IP in the GUI.
673049	FortiGate not sending its external interface IP in the IKE negotiation (Google Cloud Platform).
691178	Exchanging IPs does not work with multiple dynamic tunnels.
717082	FortiGate keeps initiating DHCP SA rekey after lifetime expires.
726450	Local out dialup IPsec traffic does not match policy-based routes.

Proxy

Bug ID	Description
604681	WAD process with SoC SSL acceleration enabled consumes more memory usage over time, which may lead to conserve mode. **Workaround**: disable SoC SSL acceleration under the firewall SSL settings.
712584	WAD memory leak causes device to go into conserve mode.

REST API

Bug ID	Description
686351	Remove blocking call to AWS meta out of `/api/v2/monitor/web-ui/state`.

Routing

Bug ID	Description
670031	LDAP traffic that originates from the FortiGate is not following SD-WAN rule.
688774	The traffic is sent out from an interface in the default route table when using `diagnose trafficctest run`.
723726	BGP session drops between virtual wire pair with auto-asic-offload enabled in policy.

Security Fabric

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

SSL VPN

Bug ID	Description
663715	icloud.com is not opening in SSL VPN web mode.
677057	SSL VPN firewall policy creation via CLI does not require setting user identity.
683823	Internal ADB Epicentro portal has issue in SSL VPN web mode.
726576	Internal webpage with JavaScript is not loading in SSL VPN web mode.
730416	Forward traffic log does not generate logs for HTTP and HTTPS services with SSL VPN web mode.

System

Bug ID	Description
555616	When NTurbo is enabled, it is unexpectedly provided with the wrong traffic direction information (from server or from client) to decide the destination for the data. This causes the traffic to be sent back to the port where it came from.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
632075	DHCP server on VLAN interface that is based on a hardware switch does not work for FortiPhone.
639861	Support FEC (forward error correction) implementations in 10G, 25G, 40G, and 100G interfaces for FG-3400E and FG-3600E.
644616	NP6 does not update session timers for traffic IPsec tunnel if established over one pure EMAC VLAN interface.
648085	Link status on peer device is not down when the admin port is down on the FortiGate.
675558	SFP port with 1G copper SFP always is up.
679035	NP6 drops, and bandwidth limited to under 10 Gbps.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
683237	Kernel panic on FG-40F after configuring FortiGuard override servers.
683299	Port group members have different speeds after the port speed is changed using a CLI script.
685674	FortiGate did not restart after restoring backup configuration.
687398	Multiple SFPs and FTLX8574D3BCL in multiple FG-1100E units have been flapping intermittently with various devices.
690287	No hardware switch function is available on FG-300E.
696556	Support `gtp-enhance-mode` (GTP-U) on FG-3815D.
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.
713529	Multiple httpsd crashes at `api_init_log_present_filter`.
713835	The BLE pin hole behavior should not be applied on FG-100F generation 1 that has no BLE built in.
715978	NTurbo does not work with EMAC VLAN interface.
721487	FortiGate often enters conserve mode due to high memory usage by httpsd process.
721789	Account profile settings changed after firmware upgrade.
732633	DNS query timeout log generated for first entry in DNS domain list when multiple domains are added.

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.

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`

722234	FSSO AD polling mode connector does not work with LDAPS.

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 FortiGate VM NIC stops responding to Azure load balancer probe when large backup files are being transferred.

WiFi Controller

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

Bug ID	Description
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.
733608	FG-5001D unable to display managed FortiAPs after upgrading.

Built-in AV engine

Resolved engine issues

Bug ID	Description
729105	The attached .DOCX file is being detected as a .ZIP file type by the AV engine when the file passes through the scanunit.
733158	AV engine crashes frequently.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
645848	FortiOS is providing self-signed CA certificate intermittently with flow-based SSL certificate inspection.
678890	IPS engine stalled, and alarm clock crash occurs at `pat_search_nocase`.
687885	Inconsistent system performance with RFC 2544 Ixia BreakingPoint testing.
708941	High CPU usage while performing changes on firewall policies.
709968	FortiGate drops UDP port 5440 traffic after rebooting both FortiGates.
712352	Firewall goes into conserve mode and IPS consumes high memory (6.00071).
720605	URL filter with exempt setting does not avoid anti virus and IPS inspection.
724400	Facebook.com website gives error in Firefox version 89 with flow mode and deep inspection.
728492	Unable to load instagram.com from Chrome browser without changing `TLS Post-Quantum Confidentiality` flag from default to enable.
729249	Web filter categorizes private IP address and local URLs as `Newly Observed Domain`.
730137	Unable to access website using policy in flow-based mode with web filter enabled.
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.

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.