FortiOS - Release Notes

Version 6.4.8

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

February 22, 2022
FortiOS 6.4.8 Release Notes
01-648-759723-20220222

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-11-18	Initial release.
2021-11-22	Updated *Fortinet Security Fabric upgrade* and *Known issues*.
2021-11-24	Updated *Product integration and support*.
2021-11-25	Updated *Special branch supported models*.
2021-12-01	Updated *Known issues*.
2021-12-06	Updated *Part numbers of unsupported FG-10xF Generation 2 models*, *Resolved issues*, and *Known issues*.
2021-12-13	Added *RDP and VNC clipboard toolbox in SSL VPN web mode* to *Special notices*. Updated *Known issues*.
2021-12-28	Updated *Resolved issues* and *Known issues*.
2022-01-10	Updated *Resolved issues* and *Known issues*.
2022-01-21	Updated *Known issues*.
2022-01-31	Updated *Resolved issues* and *Known issues*.
2022-02-07	Updated *Known issues*.
2022-02-14	Updated *Fortinet Security Fabric upgrade* and *Product integration and support*.
2022-02-22	Updated *Known issues*.

Introduction and supported models

This guide provides release information for FortiOS 6.4.8 build 1914.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.8 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 branch supported models

The following models are released on a special branch of FortiOS 6.4.8. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1914.

FG-80F-POE	is released on build 5042.
FG-81F-POE	is released on build 5042.
FG-1800F	is released on build 6165.
FG-1801F	is released on build 6165.
FG-2600F	is released on build 6165.

FG-2601F	is released on build 6165.
FG-4200F	is released on build 6165.
FG-4201F	is released on build 6165.
FG-4400F	is released on build 6165.
FG-4401F	is released on build 6165.
FWF-80F-2R	is released on build 5042.
FWF-81F-2R	is released on build 5042.
FWF-81F-2R-POE	is released on build 5042.

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 unsupported FG-10xF Generation 2 models

The following part numbers are Generation 2 models that do not support FortiOS 6.4.7 and 6.4.8:

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

RDP and VNC clipboard toolbox in SSL VPN web mode

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

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

- FortiAnalyzer 6.4.7
- FortiManager 6.4.7
- FortiClient EMS 6.4.3 build 1600 or later
- FortiClient 6.4.3 build 1608 or later
- FortiAP 6.4.4 build 0456 or later
- FortiSwitch 6.4.5 build 0461 or later

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

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

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.8. When Security Fabric is enabled in FortiOS 6.4.8, all FortiGate devices must be running FortiOS 6.4.8.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.8 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 6.4.8 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 6.4.8 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 6.4.8 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 6.4.8, 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 6.4.8.

To configure `local-access` profile:

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

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

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

FortiGate VM with V-license

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

To enable `split-vdom`:

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

FortiGate VM firmware

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

Citrix Hypervisor 8.1 Express Edition

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

Linux KVM

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

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

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

VMware ESX and ESXi

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

Firmware image checksums

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

FortiGuard update-server-location setting

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

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

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

To set FortiGuard `update-server-location`:

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

FortiView widgets

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

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

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

WanOpt configuration changes in 6.4.0

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

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

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
```

```
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

WanOpt and web cache statistics

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

IPsec interface MTU value

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

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

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

HA role wording changes

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

Virtual WAN link member lost

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

Enabling match-vip in firewall policies

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

Hardware switch members configurable under system interface list

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

Product integration and support

The following table lists FortiOS 6.4.8 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 13. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. FortiOS 6.4.8 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 13. 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 13 and Fortinet Security Fabric upgrade on page 13. 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 0302 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 4.2 version.
AV Engine	• 6.00164
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 6.4.8. For inquires about a particular bug, please contact Customer Service & Support.

System

Bug ID	Description
750149	NP7 processors are dropping CAPWAP packets when users are authenticated using an EAP method. This happens because the EAP packets are being fragmented into two packets, and the second packet is smaller than the minimum allowed packet size.

User & Authentication

Bug ID	Description
750551	DST_Root_CA_X3 certificate is expired.
757883	FortiGate blocks expired root CA, even if the cross-signed intermediate CA of the root CA is valid.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
752134	FortiOS 6.4.8 is no longer vulnerable to the following CVE Reference: • CVE-2021-42757
752450	FortiOS 6.4.8 is no longer vulnerable to the following CVE Reference: • CVE-2021-44168

Known issues

The following issues have been identified in version 6.4.8. 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.
752420	If a .TAR.BZ2 or .TAR.GZ archive contains an archive bomb inside its compressed stream, the AV engine will time out.

DNS Filter

Bug ID	Description
748227	DNS proxy generated local out rating (FortiGuard category) queries can time out if they are triggered for the same DNS domains with the same source DNS ID.

Explicit Proxy

Bug ID	Description
607230	Percent encoding is not converted in FTP over HTTP explicit proxy.
721039	Short disconnections of streaming applications (Teams and Whereby) through explicit proxy.
747840	When configuring authentication schemes to negotiate and NTLM (mix), Firefox may not show the authentication pop-up with an explicit proxy.

Firewall

Bug ID	Description
729245	HTTP/1.0 health check should process the whole response when `http-match` is set.

Bug ID	Description
738584	Firewall is using the wrong NAT IP address to send out traffic after removing the VIP and its associated policy.
743160	SYN-ACK is dropped when application control with `auto-asic-offload` and NP acceleration are enabled in a firewall policy.
745853	FortiGate stops sending logs to Netflow traffic because the Netflow session cleanup routine runs for too long when there are many long live sessions in the cache.
746891	Auto-update script sent from FortiOS GUI has a policy ID of zero, which causes FortiManager to be out of synchronization.
754240	After a session updates its shaping policy, if the new shaping policy does not configure a per-IP shaper, the session will still use the old per-IP shaper from the previous shaping policy.
767226	When a policy denies traffic for a VIP and `send-deny-packet` is enabled, the `mappedip` is used for the RST packet's source IP instead of the external IP.

FortiView

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

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
608770	When there is no IP/IPv6 address setting for *Zone*, the GUI incorrectly displays *0.0.0.0/0.0.0.0* for *IP/Netmask* and *::/0* for *IPv6 Address*.
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**: do not click on the *OK* button. Click the *Cancel* button to close the page.
653952	*The web page cannot be found* is displayed when a dashboard ID no longer exists.

Bug ID	Description
	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.
696573	Firewall policy is not visible in GUI when using `set internet-service src enable`.
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.
720613	The event log sometimes contains duplicated lines when downloaded from the GUI.
720657	Unable to reuse link local or multicast IPv6 addresses for multiple interfaces from the GUI. **Workaround**: use the CLI.
733375	On the *VPN* > *SSL-VPN Settings* page, after clicking *Apply*, `source-address` objects become `source-address6` objects if IPv6 is enabled.
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.
742561	On the *Network* > *Interfaces* page, after upgrading to FortiOS 6.4.7, a previously valid VLAN switch VLAN ID of 0 now displays the error message *The minimum value is 2*.
743477	On the *Log & Report* > *Forward Traffic* page, filtering by the *Source* or *Destination* column with negation on the IP range does not work.
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.
750490	Firewall policy changes made in the GUI remove the replacement message group in that policy.

HA

Bug ID	Description
658839	Cloning a policy from the CLI causes the HA cluster to get out of sync.
680753	`admin-restrict-local` feature does not work on management interface in HA cluster.
711521	When HA failover happens, there is a time difference between the old secondary becoming new primary and the new primary's HA ID getting updated. If a session is created in between, the session gets a wrong HA ID, which indicates incorrectly that the session's traffic needs to be handled by new secondary.
714788	Uninterruptible upgrade might be broken in large scale environments.
717788	FGSP has problem at failover when NTurbo or offloading is enabled (IPv4) with virtual wire pair traffic.
725240	HA cluster goes out of sync due to mismatched `vpn.certificate.crl` checksum.
729607	FTP transfers drop in active-active mode in cases where expectation sessions accumulated in the secondary unit reach the maximum number (128).
732201	VDOM restore on an already configured VDOM causes high CPU sometimes on the primary.
740743	When enabling `lag-out-port-select`, both cluster units simultaneously reboot.
740933	HA goes out of synchronization when uploading a local certificate.
744826	API key (token) on the secondary device is not synchronized to the primary when `standalone-config-sync` is enabled.
746008	DNS may not resolve on the correct blade in a 6K/7K virtual cluster environment.
747270	When the HA secondary device relays logs to the primary device, it may encounter high CPU usage.
752892	PPPoE connection gets disconnected during HA failover.
757494	Unable to add a member to an aggregate interface that is down in a HA cluster.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.
665755	The global UTM profiles named with a `g-` prefix are shared between all VDOMs and logically do not belong to any VDOM. When they are changed, the ipshelper cannot always refresh its configuration because the ipshelper tries to check each VDOM profile.

Bug ID	Description
682071	IPS signatures not working with VIP in proxy mode.
739272	Users cannot visit websites with an explicit web proxy when the FortiGate enters conserve mode with `fail-open` disabled. Block pages appear with the replacement message, *IPS Sensor Triggered!*.
746467	IPS engine crashes when IPS injects packets to vNP and vNP/DPDK fails to restart (crashes and sometimes is out of service).

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.
691178	Exchanging IPs does not work with multiple dynamic tunnels.
691718	Traffic cannot pass through IPsec tunnel after FEC is enabled on server side if NAT is enabled between VPN peers.
715671	Traffic is failing on dialup VPN IKEv2 with EAP authentication.
717082	FortiGate keeps initiating DHCP SA rekey after lifetime expires.
726450	Local out dialup IPsec traffic does not match policy-based routes.
729760	The ADVPN forwarder does not currently track the shortcut query that it forwards. Shortcut queries and replies are forwarded or terminated solely based on the route lookup.
735430	TCP SYN-ACKs are silently dropped if the traffic is sourced from a dialup IPsec tunnel and UTM is enabled.
740475	Traffic cannot be sent out through IPsec VPN tunnel because SA is pushed to the wrong NP6 for platforms where NP6 is standalone. Affected models: FG-2000E and FG-2500E.
743732	If a failure happens during negotiating a shortcut IPsec tunnel, the original tunnel NAT-T setting is reset by mistake.
744598	Tunnel interface MTU settings do not work when `net-device` is enabled in phase 1.
745331	IPsec server with NP offloading drops packets with an invalid SPI during rekey.
752947	The hub sometimes allows the IKEv2 IPsec tunnel with a spoke to be established that uses an expired or revoked certificate.

Log & Report

Bug ID	Description
724827	Syslogd is using the wrong source IP when configured with `interface-select-method auto`.
731154	SSL VPN tunnel down event log (log ID 39948) is missing.
745689	Unknown interface is shown in flow-based UTM logs.
749842	The miglogd process uses high CPU when handling a web rating error log that is reported with an invalid VDOM ID.
751358	Unable to set source IP for FortiCloud unless FortiCloud is already activated.
754143	Add `srcreputation` and `dstreputation` fields in the forward traffic logs to provide the reputation level of the source and destination when the traffic matches an entry in the internet service database.

Proxy

Bug ID	Description
568905	WAD crashes due to RCX having a null value.
582464	WAD SSL crash due to wrong cipher options chosen.
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.
726999	WAD crash on `wad_hash_map_del`.
728641	SSL renegotiation fails when Firefox offers TLS 1.3, but the server decides to use TLS 1.2.
733760	Proxy inspection firewall policy with proxy AV blocks POP3 traffic of the Windows 10 built-in Mail app.
743746	WAD encounters signal 11 crash when adding user information.
744756	Web proxy forward server group could not recover sometimes if the FQDN is not resolved.
752744	Proxy-based certificate with deep inspection fails upon receipt of a large handshake message.
754969	Explicit FTP proxy chooses random destination port when the FTP client initiates an FTP session without using the default port.
764193	The three-way handshake packet that was marked as `TCP port number reused` cannot pass through the FortiGate, and the FortiGate replies with a `FIN, ACK` to the client.

REST API

Bug ID	Description
743169	Update various REST API endpoints to prevent information in other VDOMs from being leaked.
743743	httpsd crashes due to `GET /api/v2/log/.../virus/archive` request when the `mkey` is not provided.

Routing

Bug ID	Description
670031	LDAP traffic that originates from the FortiGate is not following SD-WAN rule.
693988	For DSL interface, adding static route with `set dynamic-gateway enable` does not add route to routing table.
723726	BGP session drops between virtual wire pair with auto-asic-offload enabled in policy.
724574	BFD neighborship is lost between hub and spoke. One side shows BFD as down, and other side does not show the neighbor in the list.
725322	Improve the help text for `distance` to indicate that 255 means unreachable.
729002	PIM/PIM6 does not send out unicast packet with the correct source IP if interface is not specified.
731941	`Disconnected from FortiAnalyzer` events reported when the `interface-select-method` is set to `specify`, and the `interface port_<x>` is set to an interface that does not have the highest priority in the SD-WAN interface selection.
736705	ZEBOS launcher is unable to start and crashes constantly if `aspath` has more than 80 characters in the `config router router-map > set-aspath` setting.

745856	The default SD-WAN route for the LTE wwan interface is not created.
	Workaround: add a random gateway to the wwan member.
	`config system sdwan`
	`  config members`
	`  edit 2`
	`  set interface "wwan"`
	`  set gateway 10.198.58.58`
	`  set priority 100`
	`  next`
	`  end`
	`end`

746000	Multicast streams sourced on SSL VPN client are not registered in PIM-SM.
748733	Remote IP route shows `incomplete inactive` in the routing table, which causes issues with BGP routes where the peer is the next hop.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
635183	ACI dynamic address cannot be retrieved in HA vcluster2 from SDN connector.
670451	ACI SDN connector (connected by `aci-direct`) shows `curl` error 7 when updating from second VDOM.
738344	When CSF root synchronizes a large automation setting (over 16000) to the downstream FortiGate, csfd crashes while trying to process the relay message.
741346	The variable `%%date%%` resolves into `1900-01-00` instead of actual date when the schedule trigger type is used.
742743	Security rating Issue with unused deny policies.
745263	*AV & IPS DB Update* automation trigger is not working when clicking *Update Licenses & Definitions Now* in the GUI.
746950	When an Azure network interface ID contains upper case letters, the Azure SDN connector may not retrieve that network interface.

SSL VPN

Bug ID	Description
676673	Ciphers with ARIA, AESCCM, and CHACHA cannot be banned for SSL VPN.
677057	SSL VPN firewall policy creation via CLI does not require setting user identity.
693237	DCE/RPC sessions are randomly dropped (`no session matched`).
693519	SSL VPN authentication fails for PKI user with LDAP.
695386	SAML login failure when a user belongs to multiple groups associated with multiple VPN realms.
706646	SolarWinds Orion NPM platform's web application has issues in SSL VPN web mode.
707792	SSL VPN connection breaks when deleting irrelevant CA and PKI is involved.
711974	SSL VPN bookmarks are not working correctly with multiple SD-WAN zones.
718133	In some conditions, the web mode JavaScript parser will encounter an infinite loop that will cause SSL VPN crashes.
726338	The wildcard matching method does not always work as expected because the kernel sometimes does not have the address yet.
726576	Internal webpage with JavaScript is not loading in SSL VPN web mode.

Bug ID	Description
730416	Forward traffic log does not generate logs for HTTP and HTTPS services with SSL VPN web mode.
731278	Customer internal website (ac***.sa***.com) does not load properly when connecting via SSL VPN web mode.
737341	Some links and buttons are not working properly when accessing them through SSL VPN web mode.
737894	If there are no users or groups in an SSL VPN policy, the SSL VPN daemon may crash when an FQDN is a destination address in the firewall policy.
738711	FortiClient error message is not pertinent when the client does not meet host checking requirements.
745499	In cases where a user is establishing two tunnel connections, there is a chance that the second session knocks out the first session before it is updated, which causes a session leak.
746990	RADIUS accounting messages after SSL VPN do not include the Class attribute (Group name).
747352	Internal web server page, https://te***.ss***.es:10443, is not loading properly in SSL VPN web mode.
748085	Authentication request of SSL VPN realm can now only be sent to user group, local user, and remote group that is mapped to that realm in the SSL VPN settings. The authentication request will not be applied to the user group and remote group of non-realm or other realms.
749452	SSL VPN login authentication times out if primary RADIUS server becomes unavailable.
749918	Keyboard keys do not work with RDP bookmarks when PT-BR and PT-BR-ABNT2 layouts are chosen.
752055	VNC (protocol version 3.6/3.3) connection is not working in SSL VPN web mode.
755296	SSL VPN web mode has issues accessing https://e***.or***.kr.
768994	SSL VPN crashed when closing web mode RDP after upgrading to 6.4.7.

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.
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.

Bug ID	Description
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
687398	Multiple SFPs and FTLX8574D3BCL in multiple FG-1100E units have been flapping intermittently with various devices.
696556	Support `gtp-enhance-mode` (GTP-U) on FG-3815D.
699152	QinQ (802.1ad) support needed on the following models: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3600E, and FG-3601E.
702966	There was a memory leak in the administrator login debug that caused the getty daemon to be killed.
704981	LLDP transmission fails if there are nested software switches.
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.
713835	The BLE pin hole behavior should not be applied on FG-100F generation 1 that has no BLE built in.
714805	FortiManager shows auto update for down port from FortiGate, but FortiGate event logs do not show any down port events when user shuts down the `ha monitor dev`.
715978	NTurbo does not work with EMAC VLAN interface.
716341	SFP28 port flapping when the speed is set to 10G.
716483	DNS proxy is case sensitive when resolving FQDN, which may cause DNS failure in cases where local DNS forwarder is configured.
718571	In cases where there are a lot of DHCP relay interfaces (such as 1000) and an interface is added or deleted, DHCP relay takes a long time to release and initialize all interfaces before it works again.
721487	FortiGate often enters conserve mode due to high memory usage by httpsd process.
721789	Account profile settings changed after firmware upgrade.
722547	Fragmented SKB size occurs if the tail room is too small to carry the NTurbo `vtag`, which causes packets to be dropped.
724065	`Power supply 2 DC is lost` log only appears when unplugging the power cable from power supply 2.
724779	HPE setting of NTurbo host queue is missing and causes IPS traffic to stop when HPE is enabled.
728647	DHCP discovery dropped on virtual wire pair when UTM is enabled.
729939	Multiple processes crashing at the same time causes the device's management functionality to be unavailable when the packet size is smaller than `FSAE_HEADER_SIZE(6)`.
732633	DNS query timeout log generated for first entry in DNS domain list when multiple domains are added.
732760	SNMP trap packets are sometimes not sent from the primary `ha-direct` interface to all SNMP managers after upgrading.
740649	FortiGate sends CSR configuration without double quote (") to FortiManager.

Bug ID	Description
741944	The forticron process has a memory leak if there are duplicated entries in the external IP range file.
744892	DNS query responses can be bumped when dealing with a high volume of visibility hostname log requests.
745017	`get system checksum status` should only display checksums for VDOMs the current user has permissions for.
749835	Traffic logs reports ICMP destination as unreachable for received traffic
751523	When changing mode from DHCP to static, the existing DHCP IP is kept so no CLI command is generated and sent to FortiManager.
755953	Direct CLI script from FortiManager fails due to additional `end` at the end of `diagnose debug crashlog read`.
756445	Flow-based inspection on WCCP (L2 forwarding) enabled policy with VLAN interfaces causes traffic to drop if `asic-offload` is enabled.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.
778474	dhcpd is not processing discover messages if they contain a 0 length option, such as 80 (rapid commit). The warning, `length 0 overflows input buffer`, is displayed.

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.
691838	Memory leaks and crashes observed during stress long duration performance test when using FortiToken Cloud.

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.
725327	FSSO user fails to log in with principal user name.

Bug ID	Description
739702	There are unknown user logins on the FortiGate and the logs do not have any information for the unknown user.
741403	Unknown user log in to FortiGate does not provide any information for the unknown user.
744014	LLDP neighbors cannot be seen on virtual switch ports.
755302	The fnbamd process spikes to 99% or crashes during RADIUS authentication.
765136	Dynamic objects are cleared when there is no connection between the FortiGate and FortiManager with NSX-T.

VM

Bug ID	Description
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
617046	FG-VMX manager not showing all the nodes deployed.
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
722290	Azure slow path NetVSC SoftNIC has stuck RX. If using an IPsec tunnel, use UDP/4500 for ESP protocol (instead of IP/50) when SR-IOV is enabled. On the phase 1 interface, use `set nattraversal forced`. UDP/4500 is the fast path for Azure SDN, and IP/50 is the slow path that stresses guest VMs and hypervisors to the extreme. If using cross-site IPsec data backup, use Azure VNet peering technology to build raw connectivity across the site, rather than using the default IP routing based on the assigned global IP address.
736067	NSX connector stops updating addresses sometimes.
739376	vmwd gives an error when folders are created in the vSphere web interface, and vmwd ignores the IP addresses from vApp.

VoIP

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

Web Filter

Bug ID	Description
717619	Running a remote CLI script from FortiManager can create a duplicated FortiGuard web filter category.

WiFi Controller

Bug ID	Description
662714	The `security-redirect-url` setting is missing when the `portal-type` is `auth-mac`.
677994	Newly discovered and authorized FortiAP will cause HA sync issue. On the HA secondary member, if the WTP profile has a radio in monitor mode, it will be changed to AP mode and unset the band.
727301	Unable to quarantine hosts behind FortiAP and FortiSwitch.
733608	FG-5001D is unable to display managed FortiAPs after upgrading.
748154	802.1X clients are disconnected following FortiGuard update.
748479	cw_acd is crashing with signal 11 and is causing APs to disconnect/rejoin.

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.