# FortiOS - Release Notes

Version 6.4.10

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

**FORTINET VIDEO LIBRARY**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

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

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

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

**FEEDBACK**
Email: techdoc@fortinet.com

February 13, 2024
FortiOS 6.4.10 Release Notes
01-6410-820185-20240213

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2022-08-25 | Initial release. |
| 2022-08-30 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-09-19 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-10-03 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-10-06 | Updated Resolved issues on page 27. |
| 2022-10-07 | Updated Special notices on page 9. |
| 2022-10-11 | Updated New features or enhancements on page 14 and Known issues on page 41. |
| 2022-10-17 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-10-31 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-11-14 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-11-28 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-12-13 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2022-12-28 | Added VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name on page 22. |
| 2023-01-09 | Updated Known issues on page 41. |
| 2023-02-06 | Updated Known issues on page 41. |
| 2023-02-22 | Updated Known issues on page 41. |
| 2023-02-24 | Updated Resolved issues on page 27. |
| 2023-03-21 | Updated Known issues on page 41. |
| 2023-04-03 | Updated New features or enhancements on page 14 and VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name on page 22. |
| 2023-04-24 | Updated Resolved issues on page 27 and Known issues on page 41. |
| 2023-05-03 | Updated Resolved issues on page 27. |
| 2023-05-17 | Updated Known issues on page 41. |
| 2023-05-30 | Updated SSL traffic over TLS 1.0 will not be checked and will be bypassed by default on page 11 and Known issues on page 41. |
| 2023-06-14 | Updated Known issues on page 41.<br>Added IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 12. |

| Date | Change Description |
|---|---|
| 2023-06-27 | Updated Known issues on page 41. |
| 2023-08-22 | Updated Known issues on page 41. |
| 2023-09-07 | Updated Known issues on page 41. |
| 2023-09-18 | Updated Resolved issues on page 27. |
| 2023-10-16 | Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 12 and Known issues on page 41. |
| 2023-10-31 | Updated Resolved issues on page 27. |
| 2023-12-27 | Updated Known issues on page 41. |
| 2024-01-08 | Updated Known issues on page 41. |
| 2024-02-13 | Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 12. |

# Introduction and supported models

This guide provides release information for FortiOS 6.4.10 build 2000.

For FortiOS documentation, see the Fortinet Document Library.

## Supported models

FortiOS 6.4.10 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-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, 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-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, 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-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1 |
| **FortiWiFi** | FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE |
| **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 |
| **FortiFirewall** | FFW-3980E, FFW-4200F, FFW-4400F, FFW-VM64, FFW-VM64-KVM |
| **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 6.4.10. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2000.

| | |
|---|---|
| **FFW-2600F** | is released on build 5337. |

# 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).<br>• Moved configuration script upload feature to top menu > *Configuration* > *Scripts* page.<br>• Removed GUI support for auto-script configuration (the feature is still supported in the CLI).<br>• Converted all compliance tests to security rating tests. |

# PCI passthrough ports

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

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

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

```
diagnose poe upgrade-firmware
```

# AWS-On-Demand image

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

# Azure-On-Demand image

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

# FortiClient EMS Cloud registration

FortiOS 6.4.3 and later adds full support for FortiClient EMS Cloud service.

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

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

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

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

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl block
        end
    next
end
```

  - in FortiOS 6.4.3 and later:

```
config firewall ssl-ssh-profile
    edit <name>
        config ssl
            set unsupported-ssl-negotiation block
        end
    next
end
```

# 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 and later.

# Hyperscale firewall support

FortiOS 6.4.10 supports hyperscale firewall features for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). For more information, refer to the Hyperscale Firewall Release Notes.

# CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

# IP pools and VIPs are not considered local addresses for certain FortiOS versions

For FortiOS 6.4.9 and later, 7.0.1 to 7.0.12, 7.2.0 to 7.2.5, and 7.4.0, all IP addresses used as IP pools and VIPs are not considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is not considered a destination for those IP addresses and cannot receive reply traffic at the application layer without special handling.

- This behavior affects FortiOS features in the application layer that use an IP pool as its source IP pool, including SSL VPN web mode, explicit web proxy, and the phase 1 local gateway in an interface mode IPsec VPN.
- The FortiGate will not receive reply traffic at the application layer, and the corresponding FortiOS feature will not work as desired.
- Configuring an IP pool as the source NAT IP address in a regular firewall policy works as before.

For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

# Changes in default behavior

| Bug ID | Description |
|---|---|
| 718512 | Allow policy route match in the reply direction, and improve IPv6 route search for policy route to keep the same behavior as IPv4. |

# New features or enhancements

More detailed information is available in the New Features Guide.

| Bug ID | Description |
|---|---|
| 641068 | Add support for multiple internet service matches in NGFW policy mode. Previously, the ISDB query that IPS uses for security policy matching only returned the highest priority match, which led to policy matching issues when the source or destination matched multiple internet services and a lower priority internet service was configured in a policy. |
| 718332 | In previous DARRP implementation, channel bandwidth was not considered. Now, DARRP will also consider the radio bandwidth in its channel selection, adding support for 40, 80, and 160 MHz channel bandwidth. |
| 745135 | The FortiGate will default to one of the internet service databases depending on its platform, and this database cannot be changed. |
| 753368 | Add support for 802.1X under the hardware switch interface on NP6 platforms: FG-30xE, FG-40xE, and FG-110xE. |
| 759344 | NP7 CAPWAP offloading for WiFi traffic now supports VLAN-related features such as dynamic VLANs and VLAN stacking (also called QinQ or inner VLANs). |
| 787477 | Ensure that session synchronization happens correctly in the FGCP over FGSP topology.<br>1. When the session synchronization filter is applied on FGSP, the filter will only affect sessions synchronized between the FGSP peers.<br>2. When virtual clustering is used, sessions synchronized between each virtual cluster can also be synchronized to FGSP peers. The peers' `syncvd` must all be in the same HA `vcluster`. |

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

- FortiAnalyzer 6.4.8
- FortiManager 6.4.8
- 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 6.4.10. When Security Fabric is enabled in FortiOS 6.4.10, all FortiGate devices must be running FortiOS 6.4.10.

# Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.10 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 6.4.10 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 6.4.10 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 6.4.10 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 6.4.10, 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 6.4.10.

**To configure `local-access` profile:**

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

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

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

# FortiGate VM with V-license

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

**To enable `split-vdom`:**

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

# FortiGate VM firmware

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

### Citrix Hypervisor 8.1 Express Edition

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

### Linux KVM

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

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

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

### VMware ESX and ESXi

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

# Firmware image checksums

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

# FortiGuard update-server-location setting

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

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

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

**To set FortiGuard `update-server-location`:**

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

# FortiView widgets

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

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

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

# WanOpt configuration changes in 6.4.0

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

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

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

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

## WanOpt and web cache statistics

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

## IPsec interface MTU value

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

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

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

## HA role wording changes

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

## Virtual WAN link member lost

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

## Enabling match-vip in firewall policies

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

## 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.

## VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

# Product integration and support

The following table lists FortiOS 6.4.10 product integration and support information:

| | |
|---|---|
| **Web Browsers** | • Microsoft Edge<br>• Mozilla Firefox version 103<br>• Google Chrome version 104<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **Explicit Web Proxy Browser** | • Microsoft Edge<br>• Mozilla Firefox version 74<br>• Google Chrome version 80<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **FortiManager** | See important compatibility information in Fortinet Security Fabric upgrade on page 16. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library.<br>Upgrade FortiManager before upgrading FortiGate. |
| **FortiAnalyzer** | See important compatibility information in Fortinet Security Fabric upgrade on page 16. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library.<br>Upgrade FortiAnalyzer before upgrading FortiGate. |
| **FortiClient:**<br>• **Microsoft Windows**<br>• **Mac OS X**<br>• **Linux** | • 6.4.0<br>See important compatibility information in FortiClient Endpoint Telemetry license on page 16 and Fortinet Security Fabric upgrade on page 16.<br>FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later.<br>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<br>• 5.6.0 and later |
| **FortiAP-S** | • 5.4.3 and later<br>• 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<br>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C |
| **FortiSandbox** | • 2.3.3 and later |
| **Fortinet Single Sign-On (FSSO)** | • 5.0 build 0308 and later (needed for FSSO agent support OU in group filters)<br>  • Windows Server 2019 Standard<br>  • Windows Server 2019 Datacenter<br>  • Windows Server 2019 Core<br>  • Windows Server 2016 Datacenter<br>  • Windows Server 2016 Standard<br>  • Windows Server 2016 Core<br>  • Windows Server 2012 Standard<br>  • Windows Server 2012 R2 Standard<br>  • Windows Server 2012 Core<br>  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)<br>  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)<br>  • Windows Server 2008 Core (requires Microsoft SHA2 support package)<br>  • Novell eDirectory 8.8 |
| **FortiExtender** | • 4.0.0 and later. For compatibility with latest features, use latest 4.2 version. |
| **AV Engine** | • 6.00172 |
| **IPS Engine** | • 6.00139 |
| **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<br>• Windows Hyper-V Server 2019 |
| **Open Source** | • XenServer version 3.4.3<br>• XenServer version 4.1 and later |
| **VMware** | • ESX versions 4.0 and 4.1<br>• 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 103<br>Google Chrome version 104 |
| Microsoft Windows 10 (64-bit) | Microsoft Edge<br>Mozilla Firefox version 103<br>Google Chrome version 104 |
| Ubuntu 20.04 (64-bit) | Mozilla Firefox version 103<br>Google Chrome version 104 |
| macOS Big Sur 11.0 | Apple Safari version 15<br>Mozilla Firefox version 103<br>Google Chrome version 104 |
| iOS | Apple Safari |

| Operating System | Web Browser |
|---|---|
| | Mozilla Firefox<br>Google Chrome |
| Android | Mozilla Firefox<br>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 6.4.10. To inquire about a particular bug, please contact Customer Service & Support.

## Anti Virus

| Bug ID | Description |
|---|---|
| 702646 | Re-enable JavaScript heuristic detection and fix detection blocking content despite low rating. |
| 745266 | When a proxy-based policy with AV is applied, files over 37 KB are not allowed to transfer through the PowerShell script. |
| 767816 | HTTP 200 OK is not forwarded by WAD when an AV profile is enabled in a proxy-based policy. |
| 800731 | Flow AV sends HTML files to the FortiGate Cloud Sandbox every time when HTML is not configured in file list. |

## Application Control

| Bug ID | Description |
|---|---|
| 787130 | Application control does not block FTP traffic on an explicit proxy. |
| 791294 | Empty application control logs appear in policy-based mode since 7.0.0. |

## DNS Filter

| Bug ID | Description |
|---|---|
| 692482 | DNS filter forwards the DNS status code 1 `FormErr` as status code 2 `ServFail` in cases where the redirect server responses have no question section. |
| 744572 | In multi-VDOM with default `system fortiguard` configuration, the DNS filter does not work for the non-management VDOM. |
| 796052 | If local-in and transparent requests are hashed into the same local ID list, when the DNS proxy receives a response, it finds the wrong query for requests with the same ID and domain. |

## Endpoint Control

| Bug ID | Description |
|---|---|
| 802900 | The dynamic address in a firewall policy tagged with EMS matching is not consistent. |

## Explicit Proxy

| Bug ID | Description |
|---|---|
| 664380 | When configuring explicit proxy with forward server, if `ssl-ssh-profile` is enabled in `proxy-policy`, WAD is unable to correctly learn the destination type correctly, so the destination port is set to 0, but the squid proxy server does not accept the request and returns an error. |
| 755298 | SNI `ssl-exempt` result conflicts with CN `ssl-exempt` result when SNI is an IP. |
| 765761 | Firewall with forward proxy and UTM enabled is sending TLS probe with forward proxy IP instead of real server IP. |
| 778339 | Improve logic of removing HTTP Proxy-Authorization/Authorization header to prevent user credential leaking. |
| 780211 | `diagnose wad stats policy list` output displays information for only 20 proxy policies, so not all policies are included. |
| 798954 | Cisco Webex with explicit proxy and SSL deep inspection stops working after upgrading FortiOS. |
| 816879 | When an explicit proxy is enabled with IP pools, certificate inspection probe sessions use the interface IP instead of IPs from the configured IP pool. Therefore, when an interface IP is not allowed to connect externally, the probe session fails and causes traffic to not work. |

## Firewall

| Bug ID | Description |
|---|---|
| 599638 | Get unexpected count for `established session count`, and `diagnose firewall iprope clear` does not work as expected. |
| 644638 | Policy with a Tor exit node as the source is not blocking traffic coming from Tor. |
| 675977 | The `src-ip` in the health check should be allowed to be set to the interface IP of the current VDOM. |
| 688887 | The CLI should give a warning message when changing the address type from `iprange` to `ipmask` and there is no subnet input. |
| 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. |

| Bug ID | Description |
|---|---|
| 770668 | The packet dropped counter is not incremented for `per-ip-shaper` with `max-concurrent-session` as the only criterion and offload disabled on the firewall policy. |
| 773035 | Custom services name is not displayed correctly in logs with a port range of more than 3000 ports. |
| 791735 | The number of sessions in `session_count` does not match the output from `diagnose sys session full-stat`. |
| 803270 | Unexpected value for `session_count` appears. |

## FortiView

| Bug ID | Description |
|---|---|
| 692734 | When using the *5 minutes* time period, if the FortiGate system time is 40 to 59 second behind the browser time, no data is retrieved. |
| 695347 | Add support to display security policies in real time view on the *Dashboard* > *FortiView Policies* page. |
| 701979 | On the *Dashboard* > *FortiView Web Sites_FAZ* page, many websites have an *Unrated* category, and drilling down on these results displays no data. |
| 707649 | On the *Dashboard* > *FortiView Sources* page, when filtering by source and then drilling down to sessions, the GUI API call does not set the source IP filter. |

## GUI

| Bug ID | Description |
|---|---|
| 473841 | Newly created deny policy incorrectly has logging disabled and can not be enabled when the Security Fabric is enabled. |
| 630216 | A user can browse HA secondary logs in the GUI, but when a user downloads these logs, it is the primary FortiGate logs instead. |
| 663558 | *Log Details* under *Log & Report* > *Events* displays the wrong IP address when an administrative user logs in to the web console. |
| 713529 | When a FortiGate is managed by FortiManager with FortiWLM configured, the HTTPS daemon may crash while processing some FortiWLM API requests. There is no apparent impact on the GUI operation. |
| 734773 | On the *System* > *HA* page, when *vCluster* is enabled and the management VDOM is not the root VDOM, the GUI incorrectly displays management VDOM as primary VDOM. |

| Bug ID | Description |
|---|---|
| 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. |
| 739827 | On FG-VM64-AZURE, administrator is logged out every few seconds, and the following message appears in the browser: *Some cookies are misusing the recommended "SameSite" attribute*. |
| 746953 | On the *Network* > *Interfaces* page, users cannot modify the TFTP server setting. A warning with the message *This option may not function correctly. It is already configured using the CLI attribute: tftp-server.* appears beside the *DHCP Options* entry. |
| 749451 | On the *Network* > *SD-WAN* page, the volume sent/received displayed in the charts does not match the values provided from the REST API when the RX and TX values of `diagnose sys sdwan intf-sla-log` exceed $2^{32}$-1. |
| 749843 | *Bandwidth* widget does not display traffic information for VLAN interfaces when a large number of VLAN interfaces are configured. |
| 758820 | The GUI cannot restore a CLI-encrypted configuration file saved on a TFTP server. There is no issue for unencrypted configuration files or if the file is encrypted in the GUI. |
| 763925 | GUI shows user as expired after entering a comment in guest management. |
| 787565 | When logged in as guest management administrator, the custom image shows as empty on the user information printout. |

## HA

| Bug ID | Description |
|---|---|
| 683584 | The hasync process crashed because the write buffer offset is not validated before using it. |
| 683628 | The hasync process crashes often with signal 11 in cases when a CMDB mind map file is deleted and some processes still mind map the old file. |
| 717785 | HA primary does not send anti-spam and outbreak prevention license information to the secondary. |
| 750829 | In large customer configurations, some functions may time out, which causes an unexpected failover and keeps high cmdbsvr usage for a long time. |
| 751072 | HA secondary is consistently unable to synchronize any sessions from the HA primary when the original HA primary returns. |
| 752928 | fnbamd uses `ha-mgmt-interface` for certificate related DNS queries when `ha-direct` is enabled. |
| 754599 | SCTP sessions are not fully synchronized between nodes in FGSP. |
| 760562 | hasync crashes when the size of hasync statistics packets is invalid. |
| 763214 | Firmware upgrade fails when the bandwidth between `hbdev` is reduced to 26 Mbps and lower (`Check image file integrity error!`). |

| Bug ID | Description |
|---|---|
| 764873 | FGSP cluster with UTM does not forward UDP or ICMP packets to the session owner. |
| 765619 | HA desynchronizes after user from a read-only administrator group logs in. |
| 766842 | Long wait and timeout when upgrading FG- 3000D HA cluster due to vluster2 being enabled. |
| 771389 | SNMP community name with one extra character at the end stills matches when HA is enabled. |
| 779512 | If the interface name is a number, an error occurs when that number is used as an `hbdev` priority. |
| 782769 | Unable to form HA pair when HA encryption is enabled. |
| 786592 | Failure in self-pinging towards the management IP. |
| 794707 | Get invalid IP address when creating a firewall object in the CLI; it synchronized to the secondary in FGSP `standalone-config-sync`. |
| 801872 | Unexpected HA failover on AWS A-P cluster when `ipsec-soft-dec-async` is enabled. |
| 803697 | The `ha-mgmt-interface` stops using the configured `gateway6`. |
| 813600 | FortiAnalyzer connectivity test failed on the secondary unit. |

## ICAP

| Bug ID | Description |
|---|---|
| 748574 | WAD crash related to ICAP occurs. |

## Intrusion Prevention

| Bug ID | Description |
|---|---|
| 698247 | Flow mode web filter `ovrd` crashes and socket leaks in IPS daemon. |
| 699775 | Fortinet logo is missing on web filter block page in Chrome. |
| 713508 | Low download performance occurs when SSL deep inspection is enabled on aggregate and VLAN interfaces when NTurbo is enabled. |
| 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!*. |
| 809691 | High CPU usage on IPS engine when certain flow-based policies are active. |

## IPsec VPN

| Bug ID | Description |
|---|---|
| 771935 | Offloaded transit ESP is dropped in one direction until session is deleted. |
| 773313 | FG-40F-3G4G with WWAN DHCP interface set as L2TP client shows drops in WWAN connections and does not get the WWAN IP. |
| 777476 | When FGCP and FGSP is configured, but the FGCP cluster is not connected, IKE will ignore the `resync` event to synchronize SA data to the FGSP peer. |
| 781403 | IKE is consuming excessive memory. |
| 786409 | Tunnel had one-way traffic after iked crashed. |
| 789705 | IKE crash disconnected all users at the same time. |
| 790486 | Support IPsec FGSP per tunnel failover. |
| 814366 | There are no incoming ESP packets from the hub to spoke after upgrade from 6.4.8 to 6.4.9. |
| 815253 | NP7 offloaded egress ESP traffic that was not sent out of the FortiGate. |
| 825047 | The iked process crashed. |
| 825523 | NP7 drops outbound ESP after IPsec VPN is established for some time. |

## Log & Report

| Bug ID | Description |
|---|---|
| 621329 | Mixed traffic and UTM logs are in the event log file because the current `category` in the log packet header is not big enough. |
| 702859 | *Outdated report files deleted* system event log keeps being generated. |
| 708890 | Traffic log of ZTNA HTTPS proxy and TCP forwarding is missing policy name and FortiClient ID. |
| 726231 | The default `logtraffic` setting (UTM) in a security policy unexpectedly generates a traffic log. |
| 753904 | The reportd process consumes a high amount of CPU. |
| 764478 | Logs are missing on FortiGate Cloud from the FortiGate. |
| 768626 | FortiGate does not send WELF (WebTrends Enhanced Log Format) logs. |
| 769300 | Traffic denied by security policy (NGFW policy-based mode) is shown as `action="accept"` in the traffic log. |
| 774767 | The expected reboot log is missing. |
| 776929 | When submitting files for sandbox logging in flow mode, `filetype="unknown"` is displayed for PDF, DOC, JS, RTF, ZIP, and RAR files. |

| Bug ID | Description |
|---|---|
| 793352 | NGFW policy-based application control logs are being generated, even though application control is not set in the security policy. |

## Proxy

| Bug ID | Description |
|---|---|
| 678815 | WAD crashes with signal 11 if the client sends a client hello containing a key share that does not match the key share that the server prefers. |
| 716234 | WAD signal 11 crash occurs due to web cache corruptions. |
| 717995 | Proxy mode generates untagged traffic in a virtual wire pair. |
| 723104 | Proxy mode deep inspection is causing website access problems. |
| 747915 | Deep inspection of SMTPS and POP3S starts to fail after restoring the configuration file of another device with the same model. |
| 755685 | Trend Micro client results in FortiGate illegal parameter SSL alert response because the Trend Micro client sent a ClientHello that includes extra data, which is declined by the FortiGate according to RFC 5246 7.4.1.2. |
| 763988 | When `proxy-after-tcp-handshake` is enabled, IPv6 enabled sites cannot be accessed with proxy mode and a web filter profile configured. |
| 768278 | WAD crashes frequently, authentication stops, and firewall freezes once proxy policy changes are pushed out. |
| 791662 | FortiGate is silently dropping server hello in TLS negotiation. |
| 802935 | FortiGate cannot block a virus file when using the HTTP PATCH upload method. |
| 801165 | Multiple selected files cannot be deleted in SharePoint when deep inspection is enabled in a proxy policy. |
| 802935 | FortiGate cannot block a virus file when using the HTTP PATCH upload method. |
| 803260 | Memory increase suddenly and is not released until rebooting. |
| 807332 | WAD does not forward the 302 HTTP redirect to the end client. |
| 808072 | When accessing a specific website using UTF8 content encoding (which is unexpected according to the RFC) the FortiGate blocks the traffic as an HTTP evasion when applying an AV profile with deep inspection. |
| 809970 | WAD process is causing one of the CPU cores to spike to 100%. |
| 815313 | WAD crash occurred due to a certificate validation failure. |

## Routing

| Bug ID | Description |
|---|---|
| 717086 | External resource local out traffic does not follow the SD-WAN rule and specified egress interface when the `interface-select-method` configuration in `system external-resource` is changed. |
| 724541 | One IPv6 BGP neighbor is allowed to be configured with one IPv6 address format and shows a different IPv6 address format. |
| 729621 | High CPU on hub BGPD due to hub FortiGate being unable to maintain BGP connections with more than 1000 branches when `route-reflector` is enabled. |
| 730194 | When syncing a large number of service qualities, there is a chance of accessing out-of-boundary memory, which causes the VWL daemon to crash. |
| 742648 | Health check over shortcut tunnel is dead after `auto-discovery-receiver` is disabled/enabled and VWL crash occurs. |
| 745856 | The default SD-WAN route for the LTE wwan interface is not created. |
| 759752 | FortiGate is sending malformed packets causing a BGP IPv6 peering flap when there is a large amount of IPv6 routes, and they cannot fit in one packet. |
| 762258 | When policy-based routing uses a PPPoE interface, the policy route order changes after rebooting and when the link is up/down. |
| 771052 | The `set next-hop-self-rr6 enable` parameter not effective. |
| 774112 | The `key-outbound` and `key-inbound` parameters are missing on the FG-1800F and FG-1801F. |
| 778392 | Kernel panic crash occurs after receiving new IPv6 prefix via BGP. |
| 780210 | Changing the interface weight under SD-WAN takes longer to be applied from the GUI than the CLI. |
| 790806 | FortiGate SD-WAN default route is deleted after FortiManager installation with the SD-WAN template. |
| 796409 | GUI pages related to SD-WAN rules and performance SLA take 15 to 20 seconds to load. |
| 805285 | SIP-RTP fails after a route or interface change. |
| 833399 | Static routes are incorrectly added to the routing table, even if the IPsec tunnel type is static. |

## Security Fabric

| Bug ID | Description |
|---|---|
| 686420 | Dynamic address resolution is lost when SDN connector sends `sync.callback` command to the FortiGate. |

| Bug ID | Description |
|---|---|
| 690812 | FortiGate firewall dynamic address resolution lost when SDN connector updates its cache. |
| 712155 | The security rating for *Admin Idle Timeout* incorrectly fails for a FortiAnalyzer with less than 10 minutes. |
| 717080 | csfd shows high memory usage due to the JSON object not being used properly and the reference not being released properly. |
| 718469 | Wrong timestamp printed in the event log received in email from event triggered from email alert automation stitch. |
| 724071 | Log disk usage from user information history daemon is high and can restrict the use for general logging purposes. |
| 788543 | Topology tree shows *No connection* or *Unauthorized* for FortiAnalyzer while sending log data to FortiAnalyzer. |
| 789820 | The csfd process is causing high memory usage on the FortiGate. |
| 791324 | *Test Automation Stitch* function only works on the root FortiGate, and is not working on the downstream FortiGate. |

# SSL VPN

| Bug ID | Description |
|---|---|
| 729426 | The wildcard FQDN does not always work reliably in cases where the kernel does not have the address yet. |
| 740378 | Windows FortiClient 7.0.1 cannot work with FortiOS 7.0.1 over SSL VPN when the tunnel IP is in the same subnet as one of the outgoing interfaces and NAT is not enabled. |
| 741674 | Customer internal website (https://cm***.msc****.com/x***) cannot be rendered in SSL VPN web mode. |
| 745554 | Logging in with SSO to FortiAnalyzer with SSL VPN web mode fails. |
| 749857 | Web mode and tunnel mode could not reflect the VRF setting, which causes the traffic to not pass through as expected. |
| 756753 | FQDN in firewall policy is treated case sensitive, which causes SSL VPN failure when redirecting or accessing a URL that contains capitalized characters. |
| 757726 | SSL VPN web portal does not serve updated certificate. |
| 759664 | Renaming the server entry configuration will break the connection between the IdP and FortiGate, which causes the SAML login for SSL VPN to not work as expected. |
| 762685 | Punycode is not supported in SSL VPN DNS split tunneling. |
| 767832 | After upgrading from 6.4.7 to 7.0.1, the `Num Lock` key is turned off on the SSL VPN webpage. |

| Bug ID | Description |
|---|---|
| 767869 | SCADA portal will not fully load with SSL VPN web bookmark. |
| 771162 | Unable to access SSL VPN bookmark in web mode. |
| 772191 | Website is not loading in SSL VPN web mode. |
| 774661 | SSL VPN web portal not loading internal webpage. |
| 774831 | Comma character (,) is acting as delimiter in authentication session decoding when CN format is `Surname, Name`. |
| 779892 | After using the recommended upgrade path from 6.2.9 to 6.4.8, the sslvpnd daemon does not start in a consolidated policy environment. |
| 781542 | Unable to access internal SSL VPN bookmark in web mode. |
| 783508 | After upgrading to 6.4.8, NLA security mode for SSL VPN web portal bookmark does not work. |
| 786179 | Cannot reach local application (dat***.btn.co.id) while using SSL VPN web mode. |
| 796768 | SSL VPN RDP is unable to connect to load-balanced VMs. |
| 801588 | After Kronos (third-party) update from 8.1.3 to 8.1.13, SSL VPN web portal users get a blank page after logging in successfully. |
| 809209 | SSL VPN process memory leak is causing the FortiGate to enter conserve mode over a short period of time. |
| 809473 | When sslvpnd debugs are enabled, the SSL VPN process crashes more often. |
| 816716 | sslvpnd crashed when deleting a VLAN interface. |

## Switch Controller

| Bug ID | Description |
|---|---|
| 774848 | Bulk MAC addresses deletions on FortiSwitch is randomly causing all wired clients to disconnect at the same time and reconnect. |
| 777611 | NAC configuration not updating correctly on all managed switch ports. |
| 807403 | A switch is missing from the *Managed FortiSwitch* topology view (REST API has the data). |

## System

| Bug ID | Description |
|---|---|
| 623775 | newcli daemon crash due to FortiToken Mobile user token activation email processing. |

| Bug ID | Description |
|---|---|
| 666438 | The iotd daemon has problems connecting to an anycast server when `fortiguard-anycast` is disabled. |
| 679059 | The ipmc_sensord process is killed multiple times when the CPU or memory usage is high. |
| 682681 | DSL line takes a long time to synchronize. |
| 699721 | Running `diagnose hardware test network` on FWF-60F needs cable setup adjustment. |
| 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. |
| 712321 | Multiple ports flapping when a single interface is manually brought up. Affected platforms: FG-3810D and FG-3815D. |
| 716250 | Incorrect bandwidth utilization traffic widget for VLAN interface based on LACP interface. |
| 717791 | Running `execute restore vmlicense tftp` fails and displays `tftp: bind: Address already in use` message. |
| 718307 | Verizon LTE connection is not stable, and the connection may drop after a few hours. |
| 724451 | Upgrading to 6.4 removes regular VDOM links with `npuX_vlink` naming scheme. |
| 729078 | Verizon LTE connection is not stable, and the connection may drop after a few hours. |
| 738423 | Unable to create a hardware switch with no member. |
| 749613 | Unable to save configuration changes and get `failed: No space left on device` error on FG-61E, FG-81E, and FG-101E. |
| 750171 | Legitimate traffic is unable to go through with NP6 `synproxy` enabled. |
| 750533 | The cmdbsvr crashes when accessing an invalid `firewall vip` mapped IP that causes traffic to stop traversing the FortiGate. |
| 751044 | PSU alarm log and SNMP trap are added for FG-20xF and FGR-60F models. |
| 751870 | User should be disallowed from sending an alert email from a customized address if the email security compliance check fails. |
| 753912 | FortiGate calculates faulty FDS weight with DST enabled. |
| 757478 | Kernel panic results in reboot due the size of inner Ethernet header and IP header not being checked properly when the SKB is received by the VXLAN interface. |
| 764252 | On FG-100F, no event is raised for PSU failure and the diagnostic command is not available. |
| 764483 | After restoring the VDOM configuration, `Interface <VLAN> not found in the list!` is present for VLANs on the aggregate interface. |
| 771267 | Zone transfer with FortiGate as primary DNS server fails if the FortiGate has more than 241 DNS entries. |
| 771331 | Incorrect bandwidth utilization traffic widget for VLAN interface on NP6 platforms. |
| 773702 | FortiGate running startup configuration is not saved on flash drive. |

| Bug ID | Description |
|---|---|
| 775529 | Hardware switch is not passing VRRP packets. |
| 778116 | Restricted VDOM user is able to access the root VDOM. |
| 778794 | Incorrect values in NP7/hyperscale DoS policy anomaly logs. For packet rate-based meter log, the repeated numbers do not reflect the amount of dropped packets for a specific anomaly/attack; for the session counter meter log, the `pps` number is negative. |
| 779523 | Negative `tunnel_count` in `diagnose firewall gtp profile list` for FGSP peer. |
| 787595 | FFDB cannot be updated with `exec update-now` or `execute internet-service refresh` after upgrading the firmware in a large configuration. |
| 792544 | A request is made to the remote authentication server before checking `trusthost`. |
| 796398 | BPDUs packets are blocked even though STF forwarding is enabled on FG-800D in transparent mode (UTP and SFP). |
| 799255 | Any configuration changes on FG-2601F causes cmbdr crash with signal 6 and traffic to stop flowing. |
| 801410 | Hostname is not resolved when adding multiple domain lists. |
| 801474 | DHCP IP lease is flushed within the lease time. |
| 801985 | Kernel panic occurs when a virtual switch with VLAN is created, and another port is configured with a trunk. |
| 802917 | PPPoE virtual tunnel drops traffic after logon credentials are changed. |
| 809366 | FG-40F with STP enabled on a hardware switch creates a loop after upgrading to 6.4.9. |
| 811329 | The kernel crashes and forces a system reboot a few times a month in an IPsec setup with thousands of tunnels. |
| 812499 | When traffic gets offloaded, an incorrect MAC address is used as a source. |
| 813606 | DHCP relay offers to iPhones is blocked by the FortiGate. |
| 816278 | Memory increase due to iked process. |
| 824464 | CMDB checksum is not updated when a certificate is renewed over CMP, causing a FortiManager failure to synchronize with the certificate. |

# Upgrade

| Bug ID | Description |
|---|---|
| 730245 | When upgrading from 6.2.9 to 6.4.6, a `set client-cert-request inspect` parse error occurs and the parameter is set to `bypass` after the upgrade. |
| 757660 | ISDB objects are obsolete after upgrading to 6.4.6, which blocked FortiGuard access using the root VDOM. |

| Bug ID | Description |
|---|---|
| 790823 | VDOM links configuration is lost after upgrading. |

## User & Authentication

| Bug ID | Description |
|---|---|
| 624167 | FortiToken Mobile push notification not working with dynamic WAN IP service provider. |
| 754725 | After updating the FSSO DC agent to version 5.0.0301, the DC agent keeps crashing on Windows 2012 R2 and 2016, which causes lsass.exe to reboot. |
| 756763 | In the email collection captive portal, a user can click *Continue* without selecting the checkbox to accept the terms and disclaimer agreement. |
| 777004 | Local users named pop or map do not work as expected when trying to add then as sources in a firewall policy. |

## VM

| Bug ID | Description |
|---|---|
| 721439 | Problems occur when switching between HA broadcast heartbeat to unicast heartbeat and vice versa. |
| 750889 | DHCP relay fails when VMs on different VLAN interfaces use the same transaction ID. |
| 781879 | FortiFlex license activation failed to be applied to FortiGate VM in HA. Standalone mode is OK. |
| 794290 | Failed to load FFW-VM; `cw_acd: can not find board mac from interfaces` error displayed in console. |
| 799536 | Data partition is almost full on FG-VM64 platforms. |
| 800473 | FG-VM64 deployed with 6.4 loses configuration and license after upgrading to 7.2.1 (no issue if deployed with 7.0). |

## VoIP

| Bug ID | Description |
|---|---|
| 794517 | VoIP daemon memory leak occurs when the following conditions are met:<br>• The SIP call is on top of the IPsec tunnel.<br>• The call fails before the setup completes (session gets closed in a state earlier than `VOIP_SESSION_STATE_RUNNING`). |

## WiFi Controller

| Bug ID | Description |
|---|---|
| 783209 | After upgrading FortiOS from 6.2 to 6.4, a new `arrp-profile` (`arrp-default`) is added as a static entry. FortiManager cannot install the configuration to a managed FortiGate when trying to purge the `arrp-profile` table. |
| 790367 | FWF-60F has kernel panic and reboots by itself every few hours. |
| 791761 | CAPWAP tunnel traffic over WPA2-Enterprise SSID is dropped when offloading is enabled on FG-1800F. |
| 801259 | CLI script from FortiManager with two commands fails, but succeeds with one command. |

## Common Vulnerabilities and Exposures

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

| Bug ID | CVE references |
|---|---|
| 764221 | FortiOS 6.4.10 is no longer vulnerable to the following CVE Reference:<br>• CVE-2021-43206 |
| 800259 | FortiOS 6.4.10 is no longer vulnerable to the following CVE Reference:<br>• CVE-2022-29055 |
| 811492 | FortiOS 6.4.10 is no longer vulnerable to the following CVE Reference:<br>• CVE-2022-35842 |
| 819640 | FortiOS 6.4.10 is no longer vulnerable to the following CVE Reference:<br>• CVE-2022-30307 |
| 825695 | FortiOS 6.4.10 is no longer vulnerable to the following CVE Reference:<br>• CVE-2022-35843 |

# Known issues

The following issues have been identified in version 6.4.10. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

## Explicit Proxy

| Bug ID | Description |
|---|---|
| 803228 | When converting an explicit proxy session to SSL redirect, traffic may be interrupted inadvertently in some situations. |

## Firewall

| Bug ID | Description |
|---|---|
| 719311 | On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic.<br>**Workaround**: rename the custom section to unique name between IPv4 and IPv6 policies. |
| 770541 | Within the *Policy & Objects* menu, the firewall, DoS, and traffic shaping policy pages take around five seconds to load when the FortiGate cannot reach the FortiGuard DNS servers.<br>**Workaround**: set the DNS server to the FortiGuard DNS server. |
| 843554 | If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI.<br>This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.<br>**Workaround**: create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if `ALL` is the first firewall service in the list:<br>`config firewall service custom`<br>`edit "unused"`<br>`set tcp-portrange 1`<br>`next`<br>`move "unused" before "ALL"`<br>`end` |

# 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. |
| 602397 | Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches. |
| 653952 | *The web page cannot be found* is displayed when a dashboard ID no longer exists.<br>**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.<br>**Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs. |
| 743477 | On the *Log & Report* > *Forward Traffic* page, filtering by the *Source* or *Destination* column with negation on the IP range does not work. |

# HA

| Bug ID | Description |
|---|---|
| 771999 | Sessions not synchronized to HA secondary on an FGSP and FGCP combined setup. |
| 779180 | FGSP does not synchronize the `helper-pmap` expectation session. |
| 838541 | HA is out-of-sync due to `certificate local` in FGSP standalone cluster. |

## Hyperscale

| Bug ID | Description |
|---|---|
| 734305 | In the GUI, an FQDN or ISDB can be selected for a DoS policy, which is not supported (an error message appears). The CLI shows the correct options. |
| 760560 | The timestamp on the hyperscale SPU of a deny policy (policy id 0) is incorrect. |
| 796368 | Traffic shaping profile does not seem to have an effect on TCP/UDP traffic in hyperscale. |
| 802369 | Large client IP range makes fixed allocation usage relatively limited. |

## Intrusion Prevention

| Bug ID | Description |
|---|---|
| 763736 | IPS custom signature logging shows (even after being disabled) after upgrading to FortiOS 6.4.7. |

## IPsec VPN

| Bug ID | Description |
|---|---|
| 763205 | IKE crashes after HA failover when the `enforce-unique-id` option is enabled. |
| 877161 | IPsec traffic failing from FortiGate with `Failed to find IPsec Common` error when dialup IPsec VPN tunnel has remote IP configured on the IPsec VPN interface. |

## Log & Report

| Bug ID | Description |
|---|---|
| 850642 | Logs are not seen for traffic passing through the firewall caused by numerous simultaneous configuration changes. |

## Proxy

| Bug ID | Description |
|---|---|
| 604681 | WAD process with SoC SSL acceleration enabled consumes more memory usage over time, which may lead to conserve mode.<br>**Workaround**: disable SoC SSL acceleration under the firewall SSL settings. |

## REST API

| Bug ID | Description |
|---|---|
| 759675 | `Connection failed` error occurs on FortiGate when an interface is created and updated using the API in quick succession. |

## Security Fabric

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

## SSL VPN

| Bug ID | Description |
|---|---|
| 710657 | The `dstaddr`/`dstaddr6` of an SSL VPN policy can be set to `all` when split tunnel mode is enabled and only the default portal is set. |
| 730416 | Forward traffic log does not generate logs for HTTP and HTTPS services with SSL VPN web mode. |
| 852566 | User peer feature for one group to match to multiple user peers in the authentication rules is broken. |

# 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. |
| 602141 | The extender daemon crashes on Low Encryption (LENC) FortiGates. |
| 648085 | Link status on peer device is not down when the admin port is down on the FG-500E. |
| 664856 | A VWP named .. can be created in the GUI, but it cannot be edited or deleted. |
| 666664 | Interface belonging to other VDOMs should be removed from interface list when configuring a GENEVE interface. |
| 669645 | VXLAN VNI interface cannot be used with a hardware switch. |
| 685674 | FortiGate did not restart after restoring the backup configuration via FortiManager after the following process: disable NPU offloading, change NGFW mode from profile-based to policy-based, retrieve configuration from FortiGate via FortiManager, and install the policy package via FortiManager. |
| 724085 | Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled.<br>**Workaround**: set the `auto-asic-offload` option to `disable` in the firewall policy. |
| 751715 | Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed. |
| 800333 | DoS offload does not work in 6.4.9 and the npd daemon keeps crashing if the `policy-offload-level` is set to `dos-offload` under `config system npu`. Affected platforms: NP6XLite. |
| 847077 | `Can't find xitem. Drop the response.` error appears for DHCPOFFER packets in the DHCP relay debug. |
| 850688 | FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs. |
| 879769 | If the firewall session is in check-new mode, FortiOS will not flush its NPU offload entry when there is a MAC address update of its gateway. |

# Upgrade

| Bug ID | Description |
|---|---|
| 767808 | The `asicdos` option for enabling/disabling NP6XLite DoS offloading is missing after upgrading to 6.4.9. Affected platforms: NP6XLite. |

## User & Authentication

| Bug ID | Description |
|---|---|
| 778521 | SCEP fails to renew if the local certificate name length is between 31 and 35 characters. |
| 823884 | When a search is performed on a user *(User & Authentication > User Definition* page), the search results highlight all the groups the user belongs to. |
| 853793 | FG-81F 802.1X MAC authentication bypass (MAB) failed to authenticate Cisco AP. |

## 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. |

## WiFi Controller

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

# 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.