



# FortiOS - Release Notes

Version 6.0.0

**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 COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



March 5, 2020

FortiOS 6.0.0 Release Notes

01-600-452842-20200305

# TABLE OF CONTENTS

|                                                          |           |
|----------------------------------------------------------|-----------|
| <b>Change Log</b>                                        | <b>4</b>  |
| <b>Introduction</b>                                      | <b>5</b>  |
| Supported models                                         | 5         |
| <b>Special Notices</b>                                   | <b>6</b>  |
| WAN optimization and web caching functions               | 6         |
| FortiGuard Security Rating Service                       | 6         |
| Built-in certificate                                     | 7         |
| FortiGate and FortiWiFi-92D hardware limitation          | 7         |
| FG-900D and FG-1000D                                     | 8         |
| FortiClient (Mac OS X) SSL VPN requirements              | 8         |
| FortiClient profile changes                              | 8         |
| Use of dedicated management interfaces (mgmt1 and mgmt2) | 8         |
| <b>Changes in default behavior</b>                       | <b>9</b>  |
| <b>Upgrade Information</b>                               | <b>10</b> |
| Upgrading to FortiOS 6.0.0                               | 10        |
| Physical interface inclusion in zones                    | 10        |
| Security Fabric upgrade                                  | 11        |
| Minimum version of TLS services automatically changed    | 11        |
| Downgrading to previous firmware versions                | 12        |
| Amazon AWS enhanced networking compatibility issue       | 12        |
| FortiGate VM firmware                                    | 13        |
| Firmware image checksums                                 | 13        |
| FortiGuard update-server-location setting                | 13        |
| External IP not allowed to be the same as mapped IP      | 14        |
| <b>Product Integration and Support</b>                   | <b>15</b> |
| FortiOS 6.0.0 support                                    | 15        |
| Language support                                         | 17        |
| SSL VPN support                                          | 17        |
| SSL VPN standalone client                                | 17        |
| SSL VPN web mode                                         | 18        |
| SSL VPN host compatibility list                          | 18        |
| <b>Resolved Issues</b>                                   | <b>20</b> |
| <b>Known Issues</b>                                      | <b>30</b> |
| <b>Limitations</b>                                       | <b>35</b> |
| Citrix XenServer limitations                             | 35        |
| Open source XenServer limitations                        | 35        |

# Change Log

| Date       | Change Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2018-03-29 | Initial release.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 2018-04-11 | Updated version in <i>Product Integration and Support &gt; FortiOS 6.0.0 support for FortiClient iOS and FortiClient Android and FortiClient VPN Android.</i><br>Updated version in the caution in <i>Upgrade Information &gt; Upgrading to FortiOS 6.0.0.</i><br>Deleted 368644, 369099, 404399, 408100, 412112, 415186, 422670, and 436580 from <i>Known Issues.</i><br>Updated <i>Product Integration and Support &gt; Language support</i> from <i>Spanish (Spain)</i> to <i>Spanish.</i><br>Updated 440448 in <i>Resolved Issues.</i><br>Added 481785, 481615, 481649, and 481902 to <i>Known Issues.</i> |
| 2018-04-12 | Updated FortiAnalyzer version in <i>Security Fabric upgrade</i> and added 456638 to <i>Resolved Issues.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 2018-04-13 | Updated list of devices in <i>Special Notices &gt; FortiGuard Security Rating Service.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 2018-04-27 | Added IE 11 to <i>Product Integration and Support &gt; FortiOS 6.0.0 support &gt; Explicit Web Proxy Browser.</i><br>Added <i>Upgrade Information &gt; FortiGuard update-server-location setting.</i><br>Added 485676 to <i>Known Issues.</i>                                                                                                                                                                                                                                                                                                                                                                  |
| 2018-05-29 | Added <i>Special Notices &gt; WAN optimization and web caching functions.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2018-06-20 | Deleted <i>Upgrade Information &gt; FortiGate-VM64-Azure upgrade.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2018-07-06 | Updated <i>Upgrade Information &gt; Physical interface inclusion in zones</i> section.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 2018-08-02 | Added 408100 to <i>Known Issues.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 2018-10-03 | Updated description of 469821.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2018-11-26 | Added 517996 to <i>Resolved Issues.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 2019-04-11 | Deleted 434981 from <i>Resolved Issues.</i><br>Added <i>Changes in default behavior</i> section.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 2020-03-05 | Added <i>Upgrade Information &gt; External IP not allowed to be the same as mapped IP.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

# Introduction

This document provides the following information for FortiOS 6.0.0 build 0076:

- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Limitations](#)

For FortiOS documentation, see the [Fortinet Document Library](#).

## Supported models

FortiOS 6.0.0 supports the following models.

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FortiGate</b>            | FG-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E and FG-3980E |
| <b>FortiWiFi</b>            | FWF-30D, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>FortiGate Rugged</b>     | FGR-30D, FGR-35D, FGR-60D, FGR-90D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>FortiGate VM</b>         | FG-SVM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN, FG-VM64-GCP, FG-VM64-OPC, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Pay-as-you-go images</b> | FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>FortiOS Carrier</b>      | FortiOS Carrier 6.0.0 images are delivered upon request and are not available on the customer support firmware download page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

# Special Notices

## WAN optimization and web caching functions

WAN optimization and web caching functions are removed from 60D and 90D series platforms, starting from 6.0.0 due to their limited disk size. Platforms affected are:

- FGT-60D
- FGT-60D-POE
- FWF-60D
- FWF-60D-POE
- FGT-90D
- FGT-90D-POE
- FWF-90D
- FWF-90D-POE
- FGT-94D-POE

Upon upgrading from 5.6 patches to 6.0.0, `diagnose debug config-error-log read` will show command parse error about `wanopt` and `webcache` settings.

## FortiGuard Security Rating Service

Not all FortiGate models can support running the FortiGuard Security Rating Service as a Fabric "root" device. The following FortiGate platforms can run the FortiGuard Security Rating Service when added to an existing Fortinet Security Fabric managed by a supported FortiGate mode:

- FGR-30D-A
- FGR-30D
- FGR-35D
- FGR-60D
- FGR-90D
- FGT-200D
- FGT-200D-POE
- FGT-240D
- FGT-240D-POE
- FGT-280D-POE
- FGT-30D
- FGT-30D-POE
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E

- FGT-51E
- FGT-52E
- FGT-60D
- FGT-60D-POE
- FGT-70D
- FGT-70D-POE
- FGT-90D
- FGT-90D-POE
- FGT-94D-POE
- FGT-98D-POE
- FWF-30D
- FWF-30D-POE
- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E-2R
- FWF-50E
- FWF-51E
- FWF-60D
- FWF-60D-POE
- FWF-90D
- FWF-90D-POE
- FWF-92D

## Built-in certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet\_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

## FortiGate and FortiWiFi-92D hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
  set hw-switch-ether-filter <enable | disable>
```

**When the command is enabled:**

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

**When the command is disabled:**

- All packet types are allowed, but depending on the network topology, an STP loop may result.

## FG-900D and FG-1000D

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.

## FortiClient (Mac OS X) SSL VPN requirements

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

## FortiClient profile changes

With introduction of the Fortinet Security Fabric, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

The FortiClient profile on FortiGate is for FortiClient features related to compliance, such as Antivirus, Web Filter, Vulnerability Scan, and Application Firewall. You may set the *Non-Compliance Action* setting to *Block* or *Warn*. FortiClient users can change their features locally to meet the FortiGate compliance criteria. You can also use FortiClient EMS to centrally provision endpoints. The EMS also includes support for additional features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

## 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.

# Changes in default behavior

## Firewall

FortiOS 6.0.0 introduces a change in the default behavior of SNAT in firewall policies. The following is a comparison of SNAT behavior before and after the change.

| Previous releases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 6.0.0 release                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>NAT setting under the firewall policy is the control point for the NAT behavior. In the CLI, under <code>config system setting</code>,</p> <ul style="list-style-type: none"><li>• If Central-NAT is disabled, the NAT behavior is decided by the firewall policy.</li><li>• If Central-NAT is enabled, then:<ul style="list-style-type: none"><li>• If NAT is enabled under the firewall policy, the FortiGate checks the <code>central-snat-map</code> table. If there is a match, perform the action as defined. If there is no match, use the interface IP address for NAT.</li><li>• If NAT is disabled under the firewall policy, NAT is not performed.</li></ul></li></ul> | <p>NAT setting is moved from the firewall policy to <code>central-snat-map</code> table when Central-NAT is enabled. In the CLI, under <code>config system setting</code>,</p> <ul style="list-style-type: none"><li>• If Central-NAT is disabled, the NAT behavior is decided by the firewall policy the same as in previous releases (no change).</li><li>• If Central-NAT is enabled, then:<ul style="list-style-type: none"><li>• The NAT setting is not available under the firewall policy and the NAT behavior is controlled by <code>central-snat-map</code> table. Matching rules on whether or not to NAT are decided by the <code>central-snat-map</code> table.</li></ul></li></ul> |

# Upgrade Information

## Upgrading to FortiOS 6.0.0

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*.



If you are upgrading from version 5.6.2 or 5.6.3, this caution does not apply.

Before upgrading, ensure that port 4433 is not used for `admin-port` or `admin-sport` (in `config system global`), or for `SSL VPN` (in `config vpn ssl settings`).

If you are using port 4433, you must change `admin-port`, `admin-sport`, or the `SSL VPN` port to another port number before upgrading.

---

## Physical interface inclusion in zones

Upgrading from 5.6.3 or later removes all of the members of a zone if the zone contains a physical interface and at least one of that physical interface's VLAN interfaces is removed. For example:

### Before Upgrade:

```
config system zone
  edit "Trust"
    set interface "port1" "Vlan01" "Vlan02" "Vlan03"
  next
```

### After Upgrade:

```
config system zone
  edit "Trust"
  next
```

Remove `"port1"` from the list and the upgrade will retain the VLANs.

Conditions when physical zone members are removed:

- If a physical interface has a VLAN associated (regardless of whether they are in the same zone or any zone)

Conditions when VLAN zone members are removed:

- If the parent physical interface is also set on a zone

You can use the following options to prepare for the upgrade:

- Use only physical interfaces that have no VLAN associations

Or:

- Create new VLANs in place of current physical interface zone members, and remove all physical zone members from zones using only the associated, new VLAN entries.

## Security Fabric upgrade

FortiOS 6.0.0 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.0.0
- FortiClient 6.0.0
- FortiClient EMS 6.0.0
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.4 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

Before upgrading any product, you must read the *FortiOS Security Fabric Upgrade Guide*.



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.0.0. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.0 and some running 5.6.x.

---

## Minimum version of TLS services automatically changed

Support for TLS 1.0 has been discontinued for improved security. Going forward, only TLS 1.1 and TLS 1.2 will be supported.

When you upgrade to FortiOS 6.0.0 and later, all SSL and TLS services using 1.0 are automatically upgraded to 1.1 or later. For example, the `ssl-min-version` option automatically changes during upgrade to FortiOS 6.0.0 and later. As a result, if you are using TLS 1.0 with older versions of FortiOS, you can no longer use it with FortiOS 6.0.0 and later.

## 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
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles

If you have long VDOM names, you must shorten the long VDOM names (maximum 11 characters) before downgrading:

1. Back up your configuration.
2. In the backup configuration, replace all long VDOM names with its corresponding short VDOM name.  
For example, replace `edit <long_vdom_name>/<short_name>` with `edit <short_name>/<short_name>`.
3. Restore the configuration.
4. Perform the downgrade.

## Amazon AWS enhanced networking compatibility issue

With this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 6.0.0 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.0.0 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

## FortiGate VM firmware

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

### Citrix XenServer and Open Source XenServer

- `.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

- `.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 on Hyper-V 2012. 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
```

## External IP not allowed to be the same as mapped IP

Traffic will be dropped when the IPS is enabled in a policy with a VIP that has the same external and mapped IP.

To avoid this, the kernel will disallow the configuration of the same `extip` and `mappedip` for VIPs in the CLI starting from FortiOS 6.0.0.

# Product Integration and Support

## FortiOS 6.0.0 support

The following table lists 6.0.0 product integration and support information:

|                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Web Browsers</b>                                                                                                        | <ul style="list-style-type: none"><li>• Microsoft Edge 41</li><li>• Mozilla Firefox version 59</li><li>• Google Chrome version 65</li><li>• Apple Safari version 9.1 (For Mac OS X)</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.                                                                                                                                                                                                                          |
| <b>Explicit Web Proxy Browser</b>                                                                                          | <ul style="list-style-type: none"><li>• Microsoft Edge 41</li><li>• Microsoft Internet Explorer version 11</li><li>• Mozilla Firefox version 59</li><li>• Google Chrome version 65</li><li>• Apple Safari version 9.1 (For Mac OS X)</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.                                                                                                                                                                         |
| <b>FortiManager</b>                                                                                                        | See important compatibility information in <a href="#">Security Fabric upgrade on page 11</a> . For the latest information, see <a href="#">FortiManager compatibility with FortiOS</a> in the Fortinet Document Library.<br>Upgrade FortiManager before upgrading FortiGate.                                                                                                                                                                                                                        |
| <b>FortiAnalyzer</b>                                                                                                       | See important compatibility information in <a href="#">Security Fabric upgrade on page 11</a> . For the latest information, see <a href="#">FortiAnalyzer compatibility with FortiOS</a> in the Fortinet Document Library.<br>Upgrade FortiAnalyzer before upgrading FortiGate.                                                                                                                                                                                                                      |
| <b>FortiClient:</b> <ul style="list-style-type: none"><li>• Microsoft Windows</li><li>• Mac OS X</li><li>• Linux</li></ul> | <ul style="list-style-type: none"><li>• 6.0.0</li></ul> See important compatibility information in <a href="#">Security Fabric upgrade on page 11</a> . If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.<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 5.6.0 and later are supported. |
| <b>FortiClient iOS</b>                                                                                                     | <ul style="list-style-type: none"><li>• 5.6.0 and later</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>FortiClient Android and FortiClient VPN Android</b>                                                                     | <ul style="list-style-type: none"><li>• 5.4.2 and later</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>FortiAP</b>                                                                                                             | <ul style="list-style-type: none"><li>• 5.4.2 and later</li><li>• 5.6.0 and later</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FortiAP-S</b>                              | <ul style="list-style-type: none"> <li>• 5.4.3 and later</li> <li>• 5.6.0 and later</li> </ul>                                                                                                                                                                                                                                                                                                                                                                               |
| <b>FortiSwitch OS<br/>(FortiLink support)</b> | <ul style="list-style-type: none"> <li>• 3.6.4 and later</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>FortiController</b>                        | <ul style="list-style-type: none"> <li>• 5.2.5 and later</li> </ul> <p>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C</p>                                                                                                                                                                                                                                                                                                                                              |
| <b>FortiSandbox</b>                           | <ul style="list-style-type: none"> <li>• 2.3.3 and later</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Fortinet Single Sign-On<br/>(FSSO)</b>     | <ul style="list-style-type: none"> <li>• 5.0 build 0266 and later (needed for FSSO agent support OU in group filters) <ul style="list-style-type: none"> <li>• Windows Server 2016 Datacenter</li> <li>• Windows Server 2016 Standard</li> <li>• Windows Server 2008 (32-bit and 64-bit)</li> <li>• Windows Server 2008 R2 64-bit</li> <li>• Windows Server 2012 Standard</li> <li>• Windows Server 2012 R2 Standard</li> <li>• Novell eDirectory 8.8</li> </ul> </li> </ul> |
| <b>FortiExtender</b>                          | <ul style="list-style-type: none"> <li>• 3.2.1</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>AV Engine</b>                              | <ul style="list-style-type: none"> <li>• 6.00006</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>IPS Engine</b>                             | <ul style="list-style-type: none"> <li>• 4.00012</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Virtualization Environments</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Citrix</b>                                 | <ul style="list-style-type: none"> <li>• XenServer version 5.6 Service Pack 2</li> <li>• XenServer version 6.0 and later</li> </ul>                                                                                                                                                                                                                                                                                                                                          |
| <b>Linux KVM</b>                              | <ul style="list-style-type: none"> <li>• RHEL 7.1/Ubuntu 12.04 and later</li> <li>• CentOS 6.4 (qemu 0.12.1) and later</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
| <b>Microsoft</b>                              | <ul style="list-style-type: none"> <li>• Hyper-V Server 2008 R2, 2012, and 2012 R2</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Open Source</b>                            | <ul style="list-style-type: none"> <li>• XenServer version 3.4.3</li> <li>• XenServer version 4.1 and later</li> </ul>                                                                                                                                                                                                                                                                                                                                                       |
| <b>VMware</b>                                 | <ul style="list-style-type: none"> <li>• ESX versions 4.0 and 4.1</li> <li>• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5</li> </ul>                                                                                                                                                                                                                                                                                                                                  |
| <b>VM Series - SR-IOV</b>                     | <p>The following NIC chipset cards are supported:</p> <ul style="list-style-type: none"> <li>• Intel 82599</li> <li>• Intel X540</li> <li>• Intel X710/XL710</li> </ul>                                                                                                                                                                                                                                                                                                      |

## 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 standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

### Operating system and installers

| Operating System                                             | Installer                                                                                                                 |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Linux CentOS 6.5 / 7 (32-bit & 64-bit)<br>Linux Ubuntu 16.04 | 2336. Download from the Fortinet Developer Network<br><a href="https://fndn.fortinet.net">https://fndn.fortinet.net</a> . |

Other operating systems may function correctly, but are not supported by Fortinet.



SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

## 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)   | Microsoft Internet Explorer version 11 |
| Microsoft Windows 8 / 8.1 (32-bit & 64-bit) | Mozilla Firefox version 54             |
|                                             | Google Chrome version 59               |
| Microsoft Windows 10 (64-bit)               | Microsoft Edge                         |
|                                             | Microsoft Internet Explorer version 11 |
|                                             | Mozilla Firefox version 54             |
|                                             | Google Chrome version 59               |
| Linux CentOS 6.5 / 7 (32-bit & 64-bit)      | Mozilla Firefox version 54             |
| Mac OS 10.11.1                              | Apple Safari version 9                 |
|                                             | Mozilla Firefox version 54             |
|                                             | Google Chrome version 59               |
| iOS                                         | Apple Safari                           |
|                                             | Mozilla Firefox                        |
|                                             | Google Chrome                          |
| Android                                     | Mozilla Firefox                        |
|                                             | Google Chrome                          |

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

## SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

### Supported Microsoft Windows XP antivirus and firewall software

| Product                           | Antivirus | Firewall |
|-----------------------------------|-----------|----------|
| Symantec Endpoint Protection 11   | ✓         | ✓        |
| Kaspersky Antivirus 2009          | ✓         |          |
| McAfee Security Center 8.1        | ✓         | ✓        |
| Trend Micro Internet Security Pro | ✓         | ✓        |
| F-Secure Internet Security 2009   | ✓         | ✓        |

**Supported Microsoft Windows 7 32-bit antivirus and firewall software**

| Product                                                  | Antivirus | Firewall |
|----------------------------------------------------------|-----------|----------|
| CA Internet Security Suite Plus Software                 | ✓         | ✓        |
| AVG Internet Security 2011                               |           |          |
| F-Secure Internet Security 2011                          | ✓         | ✓        |
| Kaspersky Internet Security 2011                         | ✓         | ✓        |
| McAfee Internet Security 2011                            | ✓         | ✓        |
| Norton 360™ Version 4.0                                  | ✓         | ✓        |
| Norton™ Internet Security 2011                           | ✓         | ✓        |
| Panda Internet Security 2011                             | ✓         | ✓        |
| Sophos Security Suite                                    | ✓         | ✓        |
| Trend Micro Titanium Internet Security                   | ✓         | ✓        |
| ZoneAlarm Security Suite                                 | ✓         | ✓        |
| Symantec Endpoint Protection Small Business Edition 12.0 | ✓         | ✓        |

# Resolved Issues

The following issues have been fixed in version 6.0.0. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## AntiVirus

| Bug ID | Description                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------|
| 386130 | MAPI protocol does not exist in SNMP statistics for proxy.                                                |
| 435519 | FTP AV Scanning not detecting EICARS on large files (> 3GB) in both Explicit Proxy and Transparent Proxy. |
| 445999 | 6 GB attachment for AntiVirus.                                                                            |
| 456704 | When signature update runs on FortiGate device, scanunit process says busy and drop.                      |
| 459163 | Files dropped by quarantine daemon with unknown reason.                                                   |

## Authentication & User

| Bug ID | Description                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| 409100 | Edit admin/user, enable FortiToken mobile, click <i>Send activation email</i> before saving would send an empty activation code. |
| 456638 | Wildcard remote-admin login in browser with customized password gets FGT message . . . .uses default password.                   |
| 456719 | Radius attribute NAS-IP-Address incorrectly decoded.                                                                             |
| 457883 | Certificate warnings SAN missing in Chrome when redirecting to the HTTPS captive portal even though CA certificate is trusted.   |
| 460229 | Existing terminal server sessions overridden with the last terminal server user that logged on.                                  |
| 460913 | High response time when <code>rsso-flush-ip-session</code> enabled.                                                              |
| 464186 | <code>authd</code> does not send back full certificate chain to client after re-signing certificate.                             |

## DLP

| Bug ID | Description                                                                               |
|--------|-------------------------------------------------------------------------------------------|
| 454112 | hibun file with *.exe extension is detected as exe file.                                  |
| 470412 | DLP profile to block banned words with <code>regex</code> does not work on all web sites. |

## Endpoint Control

| Bug ID | Description                                                                   |
|--------|-------------------------------------------------------------------------------|
| 439638 | Infinite Outlook security pop-ups.                                            |
| 454477 | FortiGate always send 'CONT = CONT 0 ' to FortiClient in keepalive reply msg. |

## Firewall

| Bug ID | Description                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------|
| 398024 | SLB SSL offload loading issue with form page.                                                                                   |
| 445839 | Disabled logging shows action=close traffic.                                                                                    |
| 449195 | DNAT not working for SCTP -Multi-homing Traffic.                                                                                |
| 459615 | Session count incorrect.                                                                                                        |
| 462155 | Session clash for ICMP traffic from the same source IP.                                                                         |
| 467025 | Can't create the second IPv6 VIP64 which has the same ext/int IP as the existing one but with a different port-forwarding port. |
| 468156 | Log output of the <code>poluuid</code> is invalid when using firewall authentication in policy.                                 |
| 472224 | VIP LB health check erroneous status.                                                                                           |

## FOC

| Bug ID | Description                                                                                    |
|--------|------------------------------------------------------------------------------------------------|
| 437195 | GTE - PDP update request should update the associated tunnel even when two TEIDs are the same. |

## FortiGate 800D

| Bug ID | Description                                                                 |
|--------|-----------------------------------------------------------------------------|
| 450699 | FortiGate 800D shows incorrect value for TCP NONE state session statistics. |

## FortiView

| Bug ID | Description                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------|
| 366627 | FortiView Cloud Application may display incorrect drill down <i>File and Session</i> list in the <i>Applications View</i> . |
| 437137 | When fast tracked by NP6-lite chip, traffic data does not show on FortiView.                                                |

| Bug ID | Description                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------|
| 442238 | FortiView VPN map can't display Google map (199 dialup VPN tunnel).                                           |
| 442367 | In <i>FortiView &gt; Cloud Applications</i> , when the cloud users column is empty, drill down will not load. |

## GUI

| Bug ID | Description                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| 365378 | Cannot assign <code>ha-mgmt-interface</code> IP address in the same subnet as other port from GUI.                               |
| 403146 | Slow GUI <i>Policy</i> tab with more than 600 policies.                                                                          |
| 415763 | Resizing SSL VPN portal bookmark table columns in GUI does not work properly.                                                    |
| 422413 | Use API monitor to get data for FortiToken list page.                                                                            |
| 422901 | Power disruption message when logging with <code>prof_admin</code> .                                                             |
| 443647 | Traffic shaping policy dialog cannot load if application control is disabled in feature visibility.                              |
| 448197 | Show all FSSO Logons in Firewall user monitor in 5.6 is not working as before.                                                   |
| 449209 | Cannot enter more than 31 characters in an IPv6 static route destination.                                                        |
| 449726 | <i>Archived Data</i> pane for showing an IPS packet capture data is not displayed in GUI.                                        |
| 451460 | Can't read anomaly log details on log details panel when location is set as FAZ.                                                 |
| 457378 | <i>Show Matching Logs</i> of IPv4 Policy does not work when <i>Implicit Firewall Policies</i> of Feature Visibility is disabled. |
| 459904 | Rogue AP Monitor does not show the <i>Name</i> of the AP in the <i>Detected By</i> column.                                       |
| 468207 | Unable to edit User Group, when Name contains a space.                                                                           |
| 468459 | Translation issue in <i>Countries</i> .                                                                                          |
| 474024 | VLAN interface bandwidth displaced from Web GUI not matching the real speed.                                                     |

## HA

| Bug ID | Description                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------|
| 421335 | Got one time HA sync crash when run HA scripts for FIPS-CC FGT.                                                     |
| 436585 | Issues with different hardware generation when operating in a HA cluster.                                           |
| 438374 | HA reserved management interface unable to access or ping.                                                          |
| 439152 | FGSP - standalone config sync - synchronizes BGP neighbor.                                                          |
| 441078 | The time duration of packet-transporting process stops to pre-primary device node after HA failover takes too long. |

| Bug ID | Description                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 441716 | Traffic stops when <code>load-balance-all</code> is enabled in active-active HA when <code>npu_vlink</code> is used in the path.        |
| 445140 | <code>log memory max-size</code> cannot be changed in some models' HA.                                                                  |
| 445173 | FortiGate scheduled update gets failure log messages from secondary device after upgrade.                                               |
| 446860 | Insufficient warning when uploading a config to a cluster primary device.                                                               |
| 452052 | <code>vcluster2</code> 's VMAC on VLAN Interface is not persistent after <code>vcluster1</code> failing over.                           |
| 452715 | <code>ha-mgmt-interface</code> on secondary device was overwritten when back and restore config file for cluster.                       |
| 455513 | Management VDOM's I/F address on secondary device is lost or synced with primary device's.                                              |
| 457554 | FortiGate does not send syslog after <code>ha-mgmt-interface</code> link comes back up.                                                 |
| 457877 | Packets dropped with TNS session-helper enabled on FGSP cluster.                                                                        |
| 459252 | <code>Hasync</code> , <code>Hatalk</code> , and a few other processes go to D state when creating firewall policy or editing interface. |
| 462021 | Update daemon run in HA secondary unit after upgrade.                                                                                   |
| 466379 | After HA fail-over, new primary unit uses an OSPF MD5 Authentication encrypt sequence lower than the previous sequence number.          |
| 470657 | Kernel NULL pointer deference on both the devices of FGT3700D cluster.                                                                  |
| 474961 | Some daemons should run as primary device on both units when enabling standalone config sync.                                           |

## IPS

| Bug ID | Description                                                                   |
|--------|-------------------------------------------------------------------------------|
| 443418 | User is not listed in quarantine list when "block duration" has a high value. |
| 460417 | High CPU usage caused by <code>ipsengine 03.430</code> .                      |
| 471875 | Some IPS decoder configuration is lost after reboot.                          |
| 477735 | <code>ipsengine</code> crash at signal 11.                                    |

## IPsec VPN

| Bug ID | Description                                                                              |
|--------|------------------------------------------------------------------------------------------|
| 401847 | Half of IPsec tunnels traffic lost 26 minutes after powering on a spare FG-1500D.        |
| 416102 | Traffic over IPsec VPN gets dropped after two pings when it is getting offloaded to NPU. |
| 445657 | FortiOS Traffic Selector narrowing accepts wrong proposal.                               |

| Bug ID | Description                                                                                      |
|--------|--------------------------------------------------------------------------------------------------|
| 447523 | IPsec tunnel slows down in policy by sequence view even though one phase2 selector is up.        |
| 454939 | Virtual-wire-pair config is lost after reboot when using at least one vxlan interface as member. |
| 473609 | IPsec gateway not matching for PKI user when there is a DC field in the Client Certificate.      |
| 475751 | Encrypted traffic doesn't go through the IPsec tunnel.                                           |
| 476198 | IPsec traffic sourced from FW interface not processed correctly by policy.                       |
| 476461 | IKE does not release the <code>mode-cfg</code> <code>framed-IP</code> assigned from RADIUS.      |

## Log & Report

| Bug ID | Description                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------|
| 416790 | "(no.x pattern matched)" is not logged when BWL matches envelop MAIL FROM.                                 |
| 441476 | Rolled log file is not uploaded to FTP server by <code>max-log-file-size</code> .                          |
| 444958 | <i>Configuration Attribute</i> field in system event logs has length limitation.                           |
| 445291 | Local report is unable to send to multiple recipients.                                                     |
| 445522 | <code>Local report &gt; Web Usage &gt; Top users by bandwidth</code> seems to show the download as upload. |
| 449718 | No event logged for the inactive route when one member of SD-WAN interface is down.                        |

## Proxy

| Bug ID | Description                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------|
| 390666 | WAD crash in <code>wad_alarm_sig</code> process.                                                                   |
| 403140 | Improve filtering capabilities of LDAP search Explicit Proxy with Kerberos authentication.                         |
| 423480 | WAD process crashing with signal 11.                                                                               |
| 435283 | <code>block-page-status-code</code> doesn't work for HTTP status code of the DLP replacement message.              |
| 435332 | Keepalive exempted HTTPs traffic stays in kernal and proxy.                                                        |
| 442894 | WAD memory leak.                                                                                                   |
| 444257 | SSL Deep Inspection breaks for many SSL sites using Chrome.                                                        |
| 452267 | Web radio websites cannot be opened with AV in proxy mode and inspect all enabled in the protocol options profile. |
| 456502 | Transparent explicit proxy basic authentication.                                                                   |

| Bug ID | Description                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------|
| 460183 | www.cisco.com and some other sites may re-signed by untrusted CA when SSL inspection is enabled on FortiGate. |
| 464101 | WAD crashes at signal 11.                                                                                     |
| 466294 | fnbamd is suggested to implement the re-sending mechanism when sendto error.                                  |
| 466599 | New WAD end user IP associated to credentials of previous user IP owner.                                      |
| 469640 | Firewall policy Authentication redirection URL incorrect for Web-proxy traffic.                               |
| 470580 | wad memory leak for LDAP authentication.                                                                      |
| 471189 | All of scanunit daemons are killed after proxy-policy configuration changed.                                  |
| 473019 | Web category is not able to display on Web-proxy Block Page.                                                  |
| 473976 | wad process crash continuously when enable AV proxy inspection (with 3rd party explicit proxy traffic).       |
| 476708 | Internal WAD user counter gets stuck.                                                                         |
| 477161 | High memory usage on WAD process                                                                              |
| 477957 | Users getting untrusted certificate messages/timeouts.                                                        |
| 478328 | WAD is crashing at signal 11                                                                                  |

## REST API

| Bug ID | Description                                      |
|--------|--------------------------------------------------|
| 472716 | Cannot delete entry in system.mac-address-table. |

## Router

| Bug ID | Description                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------|
| 453098 | OSPF route 0.0.0.0/1 not injected.                                                                                      |
| 454871 | OSPF process crashes with signal 11 ospf_external_lsa_refresh.                                                          |
| 454916 | WAN LLB rules do not come back in same order after failover.                                                            |
| 457886 | SD-WAN rules will match traffic not destined for SD-WAN interfaces.                                                     |
| 459640 | OSPF over IPsec tunnel not getting established after VPN restart.                                                       |
| 468189 | RP is still sending multicast packet after a prune which causes a 10 second delay in case of joining within 10 seconds. |
| 468451 | Multicast flow takes 10 seconds to be forwarded if the receiver joins the group first.                                  |

| Bug ID | Description                                                                                   |
|--------|-----------------------------------------------------------------------------------------------|
| 474083 | <i>SD-WAN Health check</i> status shows interface as down though the interface is up.         |
| 475720 | Multicast flow takes 10 seconds to be forwarded if the source registers just before the join. |
| 476370 | OSPFv3 doesn't consider Forward metric for E2 routes to ASBR with interface cost statement.   |

## SSL VPN

| Bug ID | Description                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| 399784 | URL modified incorrectly for a drop-down in application server.                                                                   |
| 424561 | SSL VPN web mode has trouble loading certain page in HTTP/HTTPS bookmark.                                                         |
| 441068 | SSL VPN stale sessions in 5.4.                                                                                                    |
| 448000 | Audit mentioned to enable device detection on SSL VPN tunnel interface ( <code>ssl.root</code> ).                                 |
| 448852 | OTP for RSA Server are truncated if they are longer than 8 digits.                                                                |
| 452068 | Getting credential errors when trying to log in to an SSL web portal bookmark.                                                    |
| 469132 | Unable to view the navigation tab when accessing the <code>http://test-wiki.intence.local/xwiki</code> via SSLVPN web based mode. |
| 471472 | SSL VPN Duo authentication iframe does not load.                                                                                  |
| 472541 | Unable to login to an internal website via SSLVPN web based mode.                                                                 |
| 473963 | Web-portal allows access only to resources based on the first matched policy and its group.                                       |
| 474530 | HTTP app not working properly via SSLVPN Web Portal.                                                                              |

## System

| Bug ID | Description                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------|
| 283952 | VLAN interface Rx bytes statistics higher than underlying aggregate interface.                         |
| 412863 | NP6 drop fragment packet with payload 15319 bytes or higher.                                           |
| 423781 | Add timeout timer to proxy SSL connections.                                                            |
| 437801 | FG-30E WAN interface MTU override drop packet issue.                                                   |
| 439126 | Auto-script using diagnose command fails with <code>Unknown action 0</code> after rebooting FortiGate. |
| 439553 | Virtual wire pair config missing after reboot.                                                         |
| 440412 | SNMP trap for per-CPU usage.                                                                           |
| 440448 | Some FortiGate models will not get IP on the LTE-modem interface using Novatel U620.                   |

| Bug ID | Description                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 441532 | Suggest to add SNMP/CLI monitoring capabilities of NP6 session table.                                                                   |
| 445859 | Support for AC330U LTE modem in 5.6/5.8 trunk.                                                                                          |
| 447284 | DNS zone transfer not working automatically after reboot or <code>dnspoxyd</code> restart if primary device is temporarily unreachable. |
| 451456 | DHCP Option 82 on FortiGate DHCP relay - RFC 3046.                                                                                      |
| 452456 | Memory leak on FG-100D secondary unit.                                                                                                  |
| 453925 | Not possible to assign an IP to a GRE interface associated with another GRE interface.                                                  |
| 456439 | No system log generated for successful admin login with <code>read_only</code> privileges.                                              |
| 460894 | All ports are randomly flapping and some them are not physically connected and not in hardware switch.                                  |
| 461370 | Auto MDIX not working if interface is set to 100/full; only in auto works.                                                              |
| 461989 | ESP traffic is not forwarded out over inter-VDOM link.                                                                                  |
| 462457 | Kernel routes learnt from old ELBC primary device never expire on worker blade that are never primary device.                           |
| 466435 | Cross NP traffic on a VLAN interface configured over Aggregate interface is not forwarded.                                              |
| 467060 | Virtual Wire Pair wrongly tag the VLAN when passing from Native VLAN to Tagged VLAN.                                                    |
| 469658 | VLAN interface configuration under VDOM is lost while restoring the <code>vdom</code> configuration.                                    |
| 469821 | In TP mode, a few packets are not captured through <code>diag sniffer packet</code> .                                                   |
| 476727 | OID values for <code>fgWebfilterStatsEntry</code> and <code>fgFortiGuardStatsTable</code> trees always return 0 as value.               |

## Upgrade

| Bug ID | Description                                                             |
|--------|-------------------------------------------------------------------------|
| 459879 | Admin read-only changed privilege to same as super-admin after upgrade. |

## Usability

| Bug ID | Description                                         |
|--------|-----------------------------------------------------|
| 423715 | Unable to paste large scripts using Putty software. |

## User & Certification

| Bug ID | Description                                                                 |
|--------|-----------------------------------------------------------------------------|
| 446477 | Quarantine users by <code>srcip</code> are not blocked if a session exists. |
| 450612 | SCEP certificate renewals timeout too quickly.                              |

## VM

| Bug ID | Description                                                                   |
|--------|-------------------------------------------------------------------------------|
| 278660 | FG-AWSONDEMAND cannot register FortiCare.                                     |
| 454420 | Azure HA A-P support.                                                         |
| 462209 | Checksum mismatch on primary device and backup FGT-VM64 (VM00) over ESXi 6.0. |
| 462648 | FOSVM on-demand does not support FMG HA configuration.                        |
| 477901 | AWS API Call breaks with longer EC2 resource IDs.                             |

## WANOPT

| Bug ID | Description                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 451639 | When <code>SSL-SSH-Profile</code> is set to <i>Protect SSL Server</i> and <code>webcache-https</code> is enabled, FortiGate negotiates with its unit's certificate. |

## Web Filter

| Bug ID | Description                                                                       |
|--------|-----------------------------------------------------------------------------------|
| 467382 | Cannot create custom categories in VDOMs when using flow-based policy-based mode. |

## WiFi

| Bug ID | Description                                                          |
|--------|----------------------------------------------------------------------|
| 467758 | Not able to pass data traffic when DLTS policy is set to clear-text. |

## Common Vulnerabilities and Exposures

| Bug ID | CVE references                                                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 452384 | <p>FortiOS 6.0.0 is no longer vulnerable to the following CVE Reference:</p> <ul style="list-style-type: none"> <li>2017-14185</li> </ul> <p>Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.</p> |

| Bug ID | CVE references                                                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 452730 | FortiOS 6.0.0 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• 2017-14186</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.                     |
| 454452 | FortiOS 6.0.0 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• 2016-2183</li><li>• 2017-13077</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information. |
| 470723 | FortiOS6.0.0 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• 2017-14185</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.                      |
| 517996 | FortiOS6.0.0 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• 2018-13376</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.                      |

# Known Issues

The following issues have been identified in version 6.0.0. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## AntiVirus

| Bug ID | Description                                                       |
|--------|-------------------------------------------------------------------|
| 451348 | Flow AV SSL traffic EICAR detection failure.                      |
| 481785 | Regular AVDB becomes 1.00000 after rebooting FortiGate.           |
| 481615 | MMDB has random version number after upgrading from 5.6.3 to 6.0. |

## Application Control

| Bug ID | Description                                                                    |
|--------|--------------------------------------------------------------------------------|
| 435951 | Traffic keeps going through the DENY NGFW policy configured with URL category. |

## Connectivity

| Bug ID | Description                                                             |
|--------|-------------------------------------------------------------------------|
| 481058 | Configuration revision control list can't be retrieved from FortiCloud. |

## FortiGate 3815D

| Bug ID | Description                                     |
|--------|-------------------------------------------------|
| 385860 | FG-3815D does not support 1GE SFP transceivers. |

## FortiSwitch-Controller/FortiLink

| Bug ID | Description                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------|
| 304199 | Using HA with FortiLink can encounter traffic loss during failover.                                                    |
| 357360 | DHCP snooping may not work on IPv6.                                                                                    |
| 408082 | Operating a dedicated hardware switch into FortiLink changes STP from <i>enable</i> to <i>disable</i> in a hidden way. |

**FortiView**

| Bug ID | Description                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------|
| 375172 | FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.                |
| 414172 | HTTPsd / DNSproxy / high CPU/memory with high rate UDP 1Byte spoofing traffic.                         |
| 460016 | In <i>Fortiview &gt; Threats</i> , drill down one level, click <i>Return</i> and the graph is cleared. |

**FortiExtender**

| Bug ID | Description                                     |
|--------|-------------------------------------------------|
| 481441 | Cannot restart FortiExtender from FortiManager. |

**GUI**

| Bug ID | Description                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 408100 | Log fields are not aligned with columns after drill down on FortiView and Log details.                                                        |
| 439185 | AV quarantine cannot be viewed and downloaded from detail panel when source is FortiAnalyzer.                                                 |
| 442231 | Link cannot show different colors based on link usage legend in logical topology real time view.                                              |
| 450919 | IPS sensor with $\geq 8192$ signature entries should not be created from GUI.                                                                 |
| 451776 | Admin GUI has limit of 10 characters for OTP.                                                                                                 |
| 454734 | Security Fabric topology page cannot show detected server for (client) LAN > LAN (server) traffic.                                            |
| 455169 | Dialup VPN phase2 selector name doesn't display on GUI.                                                                                       |
| 457378 | <i>Show Matching Logs of IPv4 Policy</i> does not work when <i>Implicit Firewall Policies of Feature Visibility</i> is disabled.              |
| 468797 | Cannot filter by date or timestamp when viewing logs from FortiCloud.                                                                         |
| 470241 | Raw logs are downloaded from the default location even if you select another log device in GUI.                                               |
| 470589 | The <i>Forward Traffic Log Details</i> panel <i>Security</i> tab does not display security log details when multiple log devices are enabled. |
| 472023 | Outbreak prevention detection makes "clean" counter increment in <i>Advanced Threat Protection Stats</i> widget.                              |
| 472037 | Changing disk usage in GUI fails.                                                                                                             |
| 473791 | Four duplicate entries are displayed in <i>WANOPT</i> peer monitor when one peer was configured.                                              |
| 479030 | Should remove <i>Any</i> interface in SD-WAN rule when you specify one or more interfaces.                                                    |
| 479468 | The link status is lost after SD-WAN GUI changes to <i>List Edit</i> .                                                                        |

| Bug ID | Description                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|
| 480544 | The <i>Policy Edit Dialog</i> shows <i>WAN-OPT</i> and <i>Web Cache</i> options even though <i>Disk Setting</i> is set at <i>Log</i> . |
| 480550 | Link monitor should not display under <i>SD-WAN Monitor</i> .                                                                          |
| 480857 | In some configurations, the interface page cannot be displayed when logged in as prof admin.                                           |
| 480931 | GUI shows wrong expiry time when interface mode is DHCP.                                                                               |
| 481031 | Cannot set Security Fabric automation destination to multiple FortiGates in GUI when creating and editing automation.                  |
| 481373 | <i>Security Rating</i> in multiple FortiGates always shows first percentile even when they get different security rating scores.       |
| 481388 | The radio button for <i>Enable Explicit FTP Proxy</i> is off in the interface editing page even though FTP proxy is enabled.           |
| 481563 | The log viewer cannot view and download IPS archive when device is FortiAnalyzer and archive panel is blank.                           |
| 481902 | When accessing <i>FortiView &gt; Websites</i> page, gets error <i>Failed to get FortiView data</i> and httpsd keeps crashing.          |

## HA

| Bug ID | Description                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|
| 451470 | Unexpected performance reduction in case of Inter-Chassis HA fail-back with enabling HA override.                                    |
| 480932 | New factory reset box fails to sync with primary device in multi-VDOM after upgrade.<br>Workaround: reboot the new secondary device. |

## IPS

| Bug ID | Description                                                                                  |
|--------|----------------------------------------------------------------------------------------------|
| 445113 | IPS engine 3.428 on FortiGate sometimes cannot detect Psiphon packets that iscan can detect. |
| 481107 | IPS Engine signal 11 crash during stress test.                                               |

## IPsec VPN

| Bug ID | Description                                                                                      |
|--------|--------------------------------------------------------------------------------------------------|
| 469798 | The interface shaping with egress shaping profile doesn't work for offloaded traffic.            |
| 481153 | IPsec configuration can't create (no pask) when re-enabling OCVPN after FortiGate factory reset. |
| 481201 | The OCVPN feature is delayed about one day after registering on FortiCare.                       |
| 481449 | OCVPN may not work if FortiGate hostname is different from the one registered on cloud.          |

## Log & Report

| Bug ID | Description                                                    |
|--------|----------------------------------------------------------------|
| 412649 | In NGFW Policy mode, FortiGate does not create webfilter logs. |

## Proxy

| Bug ID | Description                                                                             |
|--------|-----------------------------------------------------------------------------------------|
| 481649 | With user authentication, the fourth request for FTP proxy service in a row is blocked. |

## Security Fabric

| Bug ID | Description                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------|
| 403229 | In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic. |
| 411368 | In FortiView with FortiAnalyzer, the combined MAC address is displayed in the <i>Device</i> field.                       |
| 414013 | Log Settings shows <code>Internal CLI error</code> when enabling historical FortiView at the same time as disk logging.  |

## SSL VPN

| Bug ID | Description                                                          |
|--------|----------------------------------------------------------------------|
| 405239 | URL rewritten incorrectly for a specific page in application server. |

## System

| Bug ID | Description                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 295292 | If <code>private-data-encryption</code> is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key. |
| 304199 | FortiLink traffic is lost in HA mode.                                                                                                             |
| 364280 | User cannot use <code>ssh-dss</code> algorithm to login to FortiGate via SSH.                                                                     |
| 436746 | NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.                                                                     |
| 440411 | Monitor NP6 IPsec engine status.                                                                                                                  |
| 445341 | Traffic between SSID and local networks is affected when NPU acceleration is enabled.                                                             |
| 474132 | FG-51E hang under stress test since build 0050.                                                                                                   |
| 480015 | Cannot show full configuration if used before entering global,                                                                                    |
| 480831 | Wrong interface status and no info on system panel after logging in with VDOM admin.                                                              |

## Upgrade

| Bug ID | Description                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------|
| 470575 | After upgrading from 5.6.3, <code>g-sniffer-profile</code> and <code>sniffer-profile</code> exist for IPS and webfilter. |
| 473075 | When upgrading, multicast policies are lost when there is a zone member as interface.                                    |
| 477241 | Device detection is enabled on some interfaces after upgrading from 5.6.3 to 6.0.0.                                      |
| 481085 | Tolerance of <code>vpn ssl web portal</code> lost when upgrading from 5.6.3 to 6.0.0.                                    |
| 481367 | Upgrading from 5.6 webfilter local categories (rating override) will be applied to all webfilter profiles.               |
| 481408 | When upgrading from 5.6.3 to 6.0.0, the IPv6 policy is lost if there is SD-WAN member as interface.                      |

## VM

| Bug ID | Description                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------|
| 480860 | FGT_VM with evaluation license does not run security rating.                                                        |
| 485676 | The FortiGuard <code>update-server-location</code> default setting is different between hardware platforms and VMs. |

## WANOPT

| Bug ID | Description                                                            |
|--------|------------------------------------------------------------------------|
| 480823 | Unknow SSL protocol error during TLS handshake with half mode offload. |

## Web Filter

| Bug ID | Description                                            |
|--------|--------------------------------------------------------|
| 480003 | FortiGuard category does not work in NGFW mode policy. |

## WiFi

| Bug ID | Description                                                                                     |
|--------|-------------------------------------------------------------------------------------------------|
| 478458 | PMF on SSID causes application <code>hostapd (wpad_ac)</code> crash.                            |
| 481394 | Fast BSS Transition on SSID causes <code>wpad_ac</code> high CPU usage (FAP cannot be managed). |

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

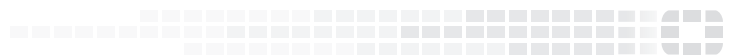
- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require 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.



**FORTINET®**



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.