



# FortiOS - Release Notes

Version 6.2.13

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



February 24, 2023

FortiOS 6.2.13 Release Notes

01-6213-880655-20230224

# TABLE OF CONTENTS

|                                                                              |           |
|------------------------------------------------------------------------------|-----------|
| <b>Change Log</b>                                                            | <b>5</b>  |
| <b>Introduction and supported models</b>                                     | <b>6</b>  |
| Supported models                                                             | 6         |
| Special branch supported models                                              | 6         |
| <b>Special notices</b>                                                       | <b>8</b>  |
| New Fortinet cloud services                                                  | 8         |
| FortiGuard Security Rating Service                                           | 8         |
| Using FortiManager as a FortiGuard server                                    | 9         |
| FortiGate hardware limitation                                                | 9         |
| CAPWAP traffic offloading                                                    | 10        |
| FortiClient (Mac OS X) SSL VPN requirements                                  | 10        |
| Use of dedicated management interfaces (mgmt1 and mgmt2)                     | 10        |
| NP4lite platforms                                                            | 10        |
| Tags option removed from GUI                                                 | 10        |
| L2TP over IPsec on certain mobile devices                                    | 10        |
| PCI passthrough ports                                                        | 11        |
| SSL traffic over TLS 1.0 will not be checked and will be bypassed by default | 11        |
| FortiGate 80D release                                                        | 11        |
| FortiGate 100D transceiver information removed                               | 11        |
| <b>Upgrade Information</b>                                                   | <b>12</b> |
| FortiGate 30E and 50E flash card space optimization                          | 12        |
| FortiClient Endpoint Telemetry license                                       | 14        |
| Fortinet Security Fabric upgrade                                             | 14        |
| Minimum version of TLS services automatically changed                        | 15        |
| Downgrading to previous firmware versions                                    | 15        |
| Amazon AWS enhanced networking compatibility issue                           | 15        |
| FortiLink access-profile setting                                             | 16        |
| FortiGate VM with V-license                                                  | 16        |
| FortiGate VM firmware                                                        | 17        |
| Firmware image checksums                                                     | 17        |
| FortiGuard update-server-location setting                                    | 18        |
| FortiView widgets                                                            | 18        |
| <b>Product integration and support</b>                                       | <b>19</b> |
| Language support                                                             | 21        |
| SSL VPN support                                                              | 21        |
| SSL VPN standalone client                                                    | 21        |
| SSL VPN web mode                                                             | 22        |
| SSL VPN host compatibility list                                              | 22        |
| <b>Resolved issues</b>                                                       | <b>24</b> |
| HA                                                                           | 24        |
| SSL VPN                                                                      | 24        |

---

|                                            |           |
|--------------------------------------------|-----------|
| System .....                               | 24        |
| Common Vulnerabilities and Exposures ..... | 24        |
| <b>Known issues .....</b>                  | <b>26</b> |
| DNS Filter .....                           | 26        |
| Explicit Proxy .....                       | 26        |
| Firewall .....                             | 26        |
| FortiView .....                            | 26        |
| GUI .....                                  | 27        |
| Intrusion Prevention .....                 | 27        |
| Log & Report .....                         | 28        |
| REST API .....                             | 28        |
| Routing .....                              | 28        |
| Security Fabric .....                      | 28        |
| SSL VPN .....                              | 29        |
| Switch Controller .....                    | 29        |
| System .....                               | 29        |
| Upgrade .....                              | 29        |
| User & Device .....                        | 30        |
| VM .....                                   | 30        |
| <b>Built-in IPS engine .....</b>           | <b>31</b> |
| Resolved engine issues .....               | 31        |
| <b>Limitations .....</b>                   | <b>32</b> |
| Citrix XenServer limitations .....         | 32        |
| Open source XenServer limitations .....    | 32        |

# Change Log

| Date       | Change Description                                   |
|------------|------------------------------------------------------|
| 2023-02-23 | Initial release.                                     |
| 2023-02-24 | Updated <a href="#">Resolved issues on page 24</a> . |

# Introduction and supported models

This guide provides release information for FortiOS 6.2.13 build 1343.

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

## Supported models

FortiOS 6.2.13 supports the following models.

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FortiGate</b>            | FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30E-MG, FG-40F, FG-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1 |
| <b>FortiWiFi</b>            | FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-40F, FWF-40F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>FortiGate Rugged</b>     | FGR-30D, FGR-35D, FGR-60F, FGR-60F-3G4G, FGR-90D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>FortiFirewall</b>        | FFW-3980E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>FortiGate VM</b>         | FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Pay-as-you-go images</b> | FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Special branch supported models

The following models are released on a special branch of FortiOS 6.2.13. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1343.

|               |                            |
|---------------|----------------------------|
| <b>FG-80D</b> | is released on build 5240. |
|---------------|----------------------------|

|                |                            |
|----------------|----------------------------|
| <b>FG-200F</b> | is released on build 7250. |
|----------------|----------------------------|

|                |                            |
|----------------|----------------------------|
| <b>FG-201F</b> | is released on build 7250. |
|----------------|----------------------------|

# Special notices

- [New Fortinet cloud services](#)
- [FortiGuard Security Rating Service](#)
- [Using FortiManager as a FortiGuard server on page 9](#)
- [FortiGate hardware limitation](#)
- [CAPWAP traffic offloading](#)
- [FortiClient \(Mac OS X\) SSL VPN requirements](#)
- [Use of dedicated management interfaces \(mgmt1 and mgmt2\)](#)
- [NP4lite platforms](#)
- [Tags option removed from GUI](#)
- [L2TP over IPsec on certain mobile devices on page 10](#)
- [PCI passthrough ports on page 11](#)
- [SSL traffic over TLS 1.0 will not be checked and will be bypassed by default on page 11](#)
- [FortiGate 80D release on page 11](#)
- [FortiGate 100D transceiver information removed on page 11](#)

## New Fortinet cloud services

FortiOS 6.2.0 introduced several new cloud-based services listed below. The new services require updates to FortiCare and Fortinet's FortiCloud single sign-on (SSO) service.

- [Overlay Controller VPN](#)
- [FortiGuard Cloud-Assist SD-WAN Interface Bandwidth Monitoring](#)
- [FortiManager Cloud](#)
- [FortiAnalyzer Cloud](#)

## 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 model:

- FGR-30D
- FGR-35D
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E
- FGT-51E

- FGT-52E
- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E
- FWF-50E-2R
- FWF-51E

## Using FortiManager as a FortiGuard server

If you use FortiManager as a FortiGuard server, and you configure the FortiGate to use a secure connection to FortiManager, you must use HTTPS with port 8888. HTTPS with port 53 is not supported.

## FortiGate 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 does 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.

## CAPWAP traffic offloading

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

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

## FortiClient (Mac OS X) SSL VPN requirements

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

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

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

## NP4lite platforms

FortiOS 6.2 and later does not support NP4lite platforms.

## Tags option removed from GUI

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

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

## L2TP over IPsec on certain mobile devices

| Bug ID | Description                                                                      |
|--------|----------------------------------------------------------------------------------|
| 459996 | Samsung Galaxy Tab A 8 and Android 9.0 crash after L2TP over IPsec is connected. |

## PCI passthrough ports

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

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

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

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

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

## FortiGate 80D release

The FortiGate 80D released in 6.2.9 and later includes the removal of the LTE modem feature using the USB port on that model.

## FortiGate 100D transceiver information removed

FortiOS 6.2.10 has removed the display of transceiver information on the *Network > Interfaces* page and the `get system interface transceiver` command.

# Upgrade Information

Supported upgrade path information is available on the [Fortinet Customer Service & Support site](#).

## To view supported upgrade path information:

1. Go to <https://support.fortinet.com>.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
  - *Current Product*
  - *Current FortiOS Version*
  - *Upgrade To FortiOS Version*
5. Click *Go*.

## FortiGate 30E and 50E flash card space optimization

On FortiGate 30 and 50 series models, the flash and /data partition may run out of space, that can cause errors after upgrade. The following models are affected:

- FortiGate 30E and 50E series
- FortiWifi 30E and 50E series
- FortiGate Rugged 30D and 35D

## To resolve this issue:

1. Install the GEOIP V2 Database on FortiGate 30 and 50 models, which uses less space on the flash card than the GEOIP v3 Database installed on other models.
2. Provide a smaller Internet Service Database (ISDB) specifically for the FortiGate 30 and 50 models, and force these models to use this smaller ISDB.
3. Move the IPS Database to the /data2 partition to reduce space on the /data partition.

## To upgrade successfully:



The output of disk spaced used in the partitions requires the use of a debug build and internal command. They are shown as reference only, based on a FortiGate 51E.

---

1. Since the initial state of the /data partition on the flash card is close to 100%, manually delete the GEOIP Database to avoid upgrade failure or loss of configuration files when upgrading the firmware:

```
# diagnose geoip delete-geoip-db  
This operation will delete the Geoip Database and reboot the system!
```

```

Only super admin has the permission with the command.
Do you want to continue? (y/n)y
Admin:admin
Password: *****
File /etc/geoip_db.gz deleted successfully.
After reboot, please update to the latest GeoDB version from FortiGuard server, with
command 'execute update-geo-ip'.
If connection to FortiGuard is not available, please upgrade the FOS firmware after
reboot.
#
The system is going down NOW !!

```

The FortiGate will automatically restart to free up space. Do not run `execute update-geo-ip` after the system reboots and before you perform the upgrade.

Note the partition size before and after the GEOIP Database is deleted.

|        |            |
|--------|------------|
| Before | 97% /data  |
|        | 93% /data2 |
| After  | 82% /data  |
|        | 93% /data2 |

2. Upgrade the FortiGate to the new firmware. Once completed, the GEOIP V2 Database is installed. Verify the installation:

```

# diagnose autoupdate versions | grep -A 2 Geography
IP Geography DB
-----
Version: 2.00114

```

3. The new firmware will force the FortiGate 30 and 50 models to use the smaller ISDB. Update the ISDB to the smaller database using FortiGuard:

```
# execute update-now
```

Once updated, additional space under the /data2 partition is available. Note the partition size before and after the smaller ISDB is installed.

|        |            |
|--------|------------|
| Before | 84% /data  |
|        | 95% /data2 |
| After  | 85% /data  |
|        | 76% /data2 |

4. Manually restart the FortiGate to allow the IPS Database to move to the /data2 partition.  
The space used in the /data and /data2 partitions are now reduced compared to before the upgrade.

## FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

## Fortinet Security Fabric upgrade

FortiOS 6.2.13 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.2.9
- FortiClient EMS 6.2.3 and later
- FortiClient 6.2.3 and later
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.11 and later

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

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



If the Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.13. When the Security Fabric is enabled in FortiOS 6.2.13, all FortiGate devices must be running FortiOS 6.2.13.

---

## Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.13 uses the `ssl-min-protocol-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.2.13 and later, the default `ssl-min-protocol-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

## Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

## Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.2.13 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.2.13 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

|      |             |      |               |
|------|-------------|------|---------------|
| C5   | Inf1        | P3   | T3a           |
| C5d  | m4.16xlarge | R4   | u-6tb1.metal  |
| C5n  | M5          | R5   | u-9tb1.metal  |
| F1   | M5a         | R5a  | u-12tb1.metal |
| G3   | M5ad        | R5ad | u-18tb1.metal |
| G4   | M5d         | R5d  | u-24tb1.metal |
| H1   | M5dn        | R5dn | X1            |
| I3   | M5n         | R5n  | X1e           |
| I3en | P2          | T3   | z1d           |

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

## FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.2.13, the `interface allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.2.13.

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

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

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

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

## FortiGate VM with V-license

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

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

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

## FortiGate VM firmware

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

### Citrix 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
```

## FortiView widgets

FortiView widgets have been rewritten in 6.2.0. FortiView widgets created in previous versions are deleted in the upgrade.

# Product integration and support

The following table lists FortiOS 6.2.13 product integration and support information:

|                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Web Browsers</b>                                                                                                                             | <ul style="list-style-type: none"><li>• Microsoft Edge</li><li>• Mozilla Firefox version 101</li><li>• Google Chrome version 102</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</li><li>• Mozilla Firefox version 101</li><li>• Google Chrome version 102</li><li>• Microsoft Internet Explorer version 11</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.                                                                                                                                                                                                  |
| <b>FortiManager</b>                                                                                                                             | See important compatibility information in <a href="#">Fortinet Security Fabric upgrade on page 14</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="#">Fortinet Security Fabric upgrade on page 14</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>• <b>Microsoft Windows</b></li><li>• <b>Mac OS X</b></li><li>• <b>Linux</b></li></ul> | <ul style="list-style-type: none"><li>• 6.2.0</li></ul> See important compatibility information in <a href="#">FortiClient Endpoint Telemetry license on page 14</a> and <a href="#">Fortinet Security Fabric upgrade on page 14</a> .<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>• 6.2.0 and later</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>FortiClient Android and FortiClient VPN Android</b>                                                                                          | <ul style="list-style-type: none"><li>• 6.2.0 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>FortiAP-U</b>                                                                                                                                | <ul style="list-style-type: none"><li>• 5.4.5 and later</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>FortiAP-W2</b>                                                                                                                               | <ul style="list-style-type: none"><li>• 5.6.0 and later</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FortiSwitch OS<br/>(FortiLink support)</b> | <ul style="list-style-type: none"> <li>• 3.6.9 and later</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>FortiController</b>                        | <ul style="list-style-type: none"> <li>• 5.2.5 and later</li> </ul> Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <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 0309 and later (needed for FSSO agent support OU in group filters)               <ul style="list-style-type: none"> <li>• Windows Server 2019 Standard</li> <li>• Windows Server 2019 Datacenter</li> <li>• Windows Server 2019 Core</li> <li>• Windows Server 2016 Datacenter</li> <li>• Windows Server 2016 Standard</li> <li>• Windows Server 2016 Core</li> <li>• Windows Server 2012 Standard</li> <li>• Windows Server 2012 R2 Standard</li> <li>• Windows Server 2012 Core</li> <li>• Windows Server 2008 (32-bit and 64-bit)</li> <li>• Windows Server 2008 R2 64-bit</li> <li>• Windows Server 2008 Core</li> <li>• Novell eDirectory 8.8</li> </ul> </li> </ul> |
| <b>FortiExtender</b>                          | <ul style="list-style-type: none"> <li>• 4.0.0 and later. For compatibility with latest features, use latest 4.0 version.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>AV Engine</b>                              | <ul style="list-style-type: none"> <li>• 6.00165</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>IPS Engine</b>                             | <ul style="list-style-type: none"> <li>• 5.00280</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Virtualization Environments</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Citrix</b>                                 | <ul style="list-style-type: none"> <li>• Hypervisor Express 8.1, build 2019-12-04</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Linux KVM</b>                              | <ul style="list-style-type: none"> <li>• Ubuntu 18.04.3 LTS</li> <li>• QEMU emulator version 4.4.4 (Debian 1:4.0+dfsg-0ubuntu9.4)</li> <li>• libvirt (libvirt) 4.0.0</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Microsoft</b>                              | <ul style="list-style-type: none"> <li>• Hyper-V Server 2019</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Open Source</b>                            | <ul style="list-style-type: none"> <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, 6.5, and 6.7</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)       | 2336. Download from the Fortinet Developer Network:<br><a href="https://fndn.fortinet.net">https://fndn.fortinet.net</a> . |
| Linux Ubuntu 16.04 / 18.04 (32-bit & 64-bit) |                                                                                                                            |

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) | Mozilla Firefox version 101<br>Google Chrome version 102                            |
| Microsoft Windows 10 (64-bit)             | Microsoft Edge<br>Mozilla Firefox version 101<br>Google Chrome version 102          |
| Ubuntu 20.04 (64-bit)                     | Mozilla Firefox version 101<br>Google Chrome version 102                            |
| macOS Monterey 12.4                       | Apple Safari version 15<br>Mozilla Firefox version 101<br>Google Chrome version 102 |
| iOS                                       | Apple Safari<br>Mozilla Firefox<br>Google Chrome                                    |
| Android                                   | Mozilla Firefox<br>Google Chrome                                                    |

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

## 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 6.2.13. To inquire about a particular bug, please contact [Customer Service & Support](#).

### HA

| Bug ID | Description                                                          |
|--------|----------------------------------------------------------------------|
| 722703 | ISDB is not updating; last update attempt is stuck at an older date. |

### SSL VPN

| Bug ID | Description                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 856316 | Browser displays an <i>Error, Feature is not available</i> message if a file larger than 1 MB is uploaded from FTP or SMB using a web bookmark, even though the file is uploaded successfully. There are no issues with downloading files. |

### System

| Bug ID | Description                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 855151 | There may be a race condition between the CMDB initializing and the customer language file loading, which causes the customer language file to be removed after upgrading. |

## Common Vulnerabilities and Exposures

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

| Bug ID | CVE references                                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 811492 | FortiOS 6.2.13 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2022-35842</li></ul> |
| 825695 | FortiOS 6.2.13 is no longer vulnerable to the following CVE Reference:                                                                  |

| Bug ID | CVE references                                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"><li>• CVE-2022-35843</li></ul>                                                                        |
| 850842 | FortiOS 6.2.13 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2022-41335</li></ul> |

# Known issues

The following issues have been identified in version 6.2.13. To inquire about a particular bug or report a bug, please contact [Customer Service & Support](#).

## DNS Filter

| Bug ID | Description                              |
|--------|------------------------------------------|
| 582374 | License shows expiry date of 0000-00-00. |

## Explicit Proxy

| Bug ID | Description                               |
|--------|-------------------------------------------|
| 540091 | Cannot access explicit FTP proxy via VIP. |

## Firewall

| Bug ID | Description                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 654356 | In NGFW policy mode, sessions are not re-validated when security policies are changed.<br><b>Workaround:</b> clear the session after policy change. |

## FortiView

| Bug ID | Description                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 635309 | When FortiAnalyzer logging is configured using an FQDN domain, the GUI displays a 500 error message on the FortiView <i>Compromised Hosts</i> page.                                                    |
| 673225 | FortiView <i>Top Traffic Shaping</i> widget does not show data for outbound traffic if the source interface's role is WAN. Data is displayed if the source interface's role is LAN, DMZ, or undefined. |

## GUI

| Bug ID | Description                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 354464 | Antivirus archive logging enabled from the CLI will be disabled by editing the antivirus profile in the GUI, even if no changes are made.                                                                                                                                                         |
| 514632 | Inconsistent reference count when using ports in HA <code>session-sync-dev</code> .                                                                                                                                                                                                               |
| 529094 | When creating an antispam block/allowlist entry, <i>Mark as Reject</i> should be grayed out.                                                                                                                                                                                                      |
| 541042 | Log viewer forwarded traffic does not support multiple filters for one field.                                                                                                                                                                                                                     |
| 584915 | OK button missing from many pages when viewed in Chrome on an Android device.                                                                                                                                                                                                                     |
| 584939 | VPN event logs are incorrectly filtered when there are two <i>Action</i> filters and one of them contains "-".                                                                                                                                                                                    |
| 602102 | Warning message is not displayed when a user configures an interface with a static IP address that is already in use.                                                                                                                                                                             |
| 602397 | Managed FortiSwitch and FortiSwitch <i>Ports</i> pages are slow to load when there are many managed FortiSwitches. This performance issue needs a fix on both FortiOS and FortiSwitch. A fix was provided in FortiOS 7.0.1 GA and FortiSwitch 7.0.1 GA.                                           |
| 621254 | When creating or editing an IPv4 policy or address group, firewall address searching does not work if there is an empty wildcard address due to a configuration error.                                                                                                                            |
| 664007 | GUI incorrectly displays the warning, <i>Botnet package update unavailable, AntiVirus subscription not found.</i> , when the antivirus entitlement is expiring within 30 days. The actual botnet package update still works within the active entitlement duration.                               |
| 672599 | After performing a search on firewall <i>Addresses</i> , the matched count over total count displayed for each address type shows an incorrect total count number. The search functionality still works correctly.                                                                                |
| 682440 | On <i>Firewall Policy</i> list, the tooltip for <i>IP Pool</i> incorrectly shows <i>Port Block Allocation</i> as being exhausted if there are expiring PBAs available to be reallocated.                                                                                                          |
| 688994 | The <i>Edit Web Filter Profile</i> page incorrectly shows that a URL filter is configured (even though it is not) if the URL filter entry has the same name as the web filter profile in the CLI.                                                                                                 |
| 695163 | When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI <i>Forward Traffic</i> log page can take time to load if there is no specific filter for the time range.<br><b>Workaround:</b> provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs. |

## Intrusion Prevention

| Bug ID | Description                             |
|--------|-----------------------------------------|
| 565747 | IPS engine 5.00027 has signal 11 crash. |

| Bug ID | Description                                                                                          |
|--------|------------------------------------------------------------------------------------------------------|
| 586544 | IPS intelligent mode not working when reflect sessions are created on different physical interfaces. |
| 587668 | IPS engine 5.00035 has signal 11 crash.                                                              |
| 590087 | When IPS pcap is enabled, traffic is intermittently disrupted after disk I/O reaches IOPS limit.     |

## Log & Report

| Bug ID | Description                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------|
| 606533 | User observes <code>FGT internal error</code> while trying to log in or activate FortiGate Cloud from the web UI. |

## REST API

| Bug ID | Description                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 584631 | REST API administrator with token unable to configure HA setting (via login session works).                                                                                                                                                   |
| 713445 | For API user tokens with CORS enabled and set to wildcard *, direct API requests using this token are not processed properly. This issue impacts FortiOS version 5.6.1 and later.<br><b>Workaround:</b> set CORS to an explicit domain.       |
| 714075 | When CORS is enabled for REST API administrators, POST and PUT requests with body data do not work with CORS due to the pre-flight requests being handled incorrectly. This only impacts newer browser versions that use pre-flight requests. |

## Routing

| Bug ID | Description                                                          |
|--------|----------------------------------------------------------------------|
| 537354 | BFD/BGP dropping when <code>outbandwidth</code> is set on interface. |

## Security Fabric

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

## SSL VPN

| Bug ID | Description                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------|
| 505986 | On IE 11, SSL VPN web portal displays blank page title <code>{{::data.portal.heading}}</code> after authentication. |

## Switch Controller

| Bug ID | Description                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------|
| 588584 | GUI should add support to allow using switch VLAN interface under a tenant VDOM on a managed switch VDOM. |
| 605864 | If the firewall is downgraded from 6.2.3 to 6.2.2, the FortiLink interface loses its CAPWAP setting.      |

## System

| Bug ID | Description                                                                        |
|--------|------------------------------------------------------------------------------------|
| 464340 | EHP drops for units with no NP service module.                                     |
| 578031 | FortiManager Cloud cannot be removed once the FortiGate has trouble with contract. |
| 595244 | There is duplicate information when checking interface references in global.       |
| 600032 | SNMP does not provide routing table for non-management VDOM.                       |
| 607565 | Interface <code>emac-vlan</code> feature does not work on SoC4 platform.           |
| 669645 | VXLAN VNI interface cannot be used with a hardware switch.                         |
| 694202 | <code>stpforward</code> does not work with LAG interfaces on a transparent VDOM.   |

## Upgrade

| Bug ID | Description                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 658664 | FortiExtender status becomes <code>discovered</code> after upgrading from 6.0.10 (build 0365).<br><b>Workaround:</b> change the <code>admin</code> from <code>discovered</code> to <code>enable</code> after upgrading.<br><pre>config extender-controller extender   edit &lt;id&gt;</pre> |

| Bug ID | Description                          |
|--------|--------------------------------------|
|        | <pre>set admin enable next end</pre> |

## User & Device

| Bug ID | Description                                                             |
|--------|-------------------------------------------------------------------------|
| 595583 | Device identification via LLDP on an aggregate interface does not work. |

## VM

| Bug ID | Description                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------|
| 587757 | FG-VM image unable to be deployed on AWS with additional HDD (st1) disk type.                                             |
| 596742 | Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.        |
| 605511 | FG-VM-GCP reboots a couple of times due to kernel panic.                                                                  |
| 608881 | IPsec VPN tunnel not staying up after failing over with AWS A-P cross-AZ setup.                                           |
| 640436 | FortiGate AWS bootstrapped from configuration does not read SAML settings.                                                |
| 668625 | During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.                           |
| 685782 | HTTPS administrative interface responds over heartbeat port on Azure FortiGate despite <code>allowaccess</code> settings. |

## Built-in IPS engine

### Resolved engine issues

| Bug ID | Description                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------|
| 590623 | Strange padding occurs in certificate after deep inspection (ICAgICAg...).                                  |
| 683066 | IPS engine crashes and consumes high CPU.                                                                   |
| 789861 | Globus file transfer traffic breaks when web filter profile is enabled along with certificate inspection.   |
| 802683 | IPS debug filter is not working.                                                                            |
| 804500 | Changes to the custom URL filter cause a network degradation that impacts customers.                        |
| 808961 | IPS engine stalled and caused packet drops.                                                                 |
| 816759 | IPS engine 5.00272 crash on <code>ovrd_ssl_read</code> .                                                    |
| 822573 | URL filter cannot be blocked if it has an IPS sensor on same firewall policy with flow inspection mode.     |
| 827253 | Only traffic to pure IPv6 is blocked, and traffic to obfuscated IPv6 is not detected by FortiOS.            |
| 836955 | Primary and secondary units of HA cluster are not accessible and drop traffic.                              |
| 848368 | IPS is causing high memory (FortiOS 6.4.8).                                                                 |
| 849030 | IPS engine <code>libips.so</code> process crashes with signal 11 at <code>sock_read_stop</code> .           |
| 855301 | IPS engine is consuming high memory.                                                                        |
| 863074 | Both <code>block</code> and <code>passthrough</code> logs are sent out by the web filter override function. |
| 873153 | URLs longer than 8000 characters are unable to get a FortiGuard rating with flow-based URL filter.          |

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

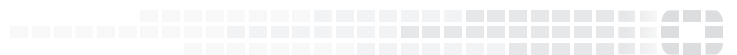
- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require 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© 2023 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.