

# Release Notes

**FortiOS 7.2.12**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



September 10, 2025

FortiOS 7.2.12 Release Notes

01-7212-1180712-20250910

# 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   | 7         |
| FortiGate 6000 and 7000 support   | 7         |
| <b>Special notices</b>  | <b>8</b>  |
| IPsec phase 1 interface type cannot be changed after it is configured                               | 8         |
| FortiGate 6000 and 7000 incompatibilities and limitations   | 8         |
| Hyperscale incompatibilities and limitations  | 9         |
| SMB drive mapping with ZTNA access proxy  | 9         |
| Console error message when FortiGate 40xF boots   | 9         |
| Hyperscale NP7 hardware limitation  | 9         |
| Changes to NP7 traffic shaping  | 10        |
| GUI cannot be accessed when using a server certificate with an RSA 1024 bit key                     | 10        |
| SSL VPN not supported on FortiGate G-series Entry-Level models                                      | 11        |
| SAML certificate verification   | 11        |
| <b>Changes in GUI behavior</b>  | <b>12</b> |
| <b>Changes in default behavior</b>  | <b>13</b> |
| <b>New features or enhancements</b>   | <b>14</b> |
| <b>Upgrade information</b>  | <b>15</b> |
| Fortinet Security Fabric upgrade  | 15        |
| Downgrading to previous firmware versions   | 17        |
| Firmware image checksums  | 17        |
| Strong cryptographic cipher requirements for FortiAP  | 17        |
| FortiGate VM VDOM licenses  | 18        |
| VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name | 18        |
| FortiGate 6000 and 7000 upgrade information   | 19        |
| Upgrade error message   | 20        |
| FortiGates with ULL ports may experience status down on active ports                                | 20        |
| SLBC FG-5001E primary blade fails to install image  | 20        |
| Admin Access Lockout Risk when upgrading or downgrading from versions with PBKDF2 support           | 21        |
| <b>Product integration and support</b>  | <b>22</b> |
| Virtualization environments   | 23        |
| Language support  | 23        |
| SSL VPN support   | 24        |
| SSL VPN web mode  | 24        |
| <b>Resolved issues</b>  | <b>25</b> |
| Firewall  | 25        |
| FortiGate 6000 and 7000 platforms   | 25        |

|  |           |
|--|-----------|
| FortiSASE .....  | 26        |
| GUI .....  | 26        |
| HA .....   | 26        |
| IPsec VPN .....  | 26        |
| Proxy .....  | 27        |
| Routing .....  | 27        |
| SSL VPN .....  | 27        |
| System .....   | 28        |
| VM .....   | 28        |
| Web Filter .....   | 28        |
| <b>Known issues .....</b>  | <b>29</b> |
| New known issues .....   | 29        |
| FortiGate 6000 and 7000 platforms .....  | 29        |
| Existing known issues .....  | 29        |
| Anti Virus .....   | 29        |
| Explicit Proxy .....   | 30        |
| FortiGate 6000 and 7000 platforms .....  | 30        |
| FortiView .....  | 32        |
| GUI .....  | 32        |
| HA .....   | 33        |
| Hyperscale .....   | 33        |
| IPsec VPN .....  | 34        |
| Proxy .....  | 34        |
| REST API .....   | 34        |
| Routing .....  | 34        |
| Security Fabric .....  | 35        |
| SSL VPN .....  | 35        |
| Switch Controller .....  | 36        |
| System .....   | 36        |
| Upgrade .....  | 37        |
| User & Authentication .....  | 37        |
| VM .....   | 37        |
| Web Filter .....   | 38        |
| WiFi Controller .....  | 38        |
| ZTNA .....   | 38        |
| <b>Built-in AV Engine .....</b>  | <b>39</b> |
| <b>Built-in IPS Engine .....</b>   | <b>40</b> |
| <b>Limitations .....</b>   | <b>41</b> |
| Citrix XenServer limitations .....   | 41        |
| Open source XenServer limitations .....  | 41        |
| Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models ..... | 41        |

# Change Log

| Date       | Change Description |
|------------|--------------------|
| 2025-09-10 | Initial release.   |

# Introduction and supported models

This guide provides release information for FortiOS 7.2.12 build 1761.

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

## Supported models

FortiOS 7.2.12 supports the following models.

|                             |   |
|-----------------------------|---|
| <b>FortiGate</b>            | FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-90G, FG-91E, FG-91G, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-120G, FG-121G, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F |
| <b>FortiWiFi</b>            | FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE   |
| <b>FortiGate Rugged</b>     | FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G  |
| <b>FortiFirewall</b>        | FFW-1801F, FFW-2600F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM   |
| <b>FortiGate VM</b>         | FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-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 7.2.12. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1761.

|                    |                           |
|--------------------|---------------------------|
| <b>FG-30G</b>      | is released on build 6666 |
| <b>FG-31G</b>      | is released on build 6666 |
| <b>FG-70G</b>      | is released on build 6665 |
| <b>FG-70G-POE</b>  | is released on build 6665 |
| <b>FG-71G</b>      | is released on build 6665 |
| <b>FG-71G-POE</b>  | is released on build 6665 |
| <b>FG-200G</b>     | is released on build 6663 |
| <b>FG-201G</b>     | is released on build 6663 |
| <b>FWF-30G</b>     | is released on build 6666 |
| <b>FWF-31G</b>     | is released on build 6666 |
| <b>FWF-70G</b>     | is released on build 6665 |
| <b>FWF-70G-POE</b> | is released on build 6665 |
| <b>FWF-71G</b>     | is released on build 6665 |

## FortiGate 6000 and 7000 support

FortiOS 7.2.12 supports the following FG-6000F, FG-7000E, and FG-7000F models:

|                 |  |
|-----------------|--|
| <b>FG-6000F</b> | FG-6001F, FG-6300F, FG-6301F, FG-6500F, FG-6501F |
| <b>FG-7000E</b> | FG-7030E, FG-7040E, FG-7060E                     |
| <b>FG-7000F</b> | FG-7081F, FG-7121F                               |

# Special notices

- [IPsec phase 1 interface type cannot be changed after it is configured on page 8](#)
- [FortiGate 6000 and 7000 incompatibilities and limitations on page 8](#)
- [Hyperscale incompatibilities and limitations on page 9](#)
- [SMB drive mapping with ZTNA access proxy on page 9](#)
- [Console error message when FortiGate 40xF boots on page 9](#)
- [Hyperscale NP7 hardware limitation on page 9](#)
- [Changes to NP7 traffic shaping on page 10](#)
- [GUI cannot be accessed when using a server certificate with an RSA 1024 bit key on page 10](#)
- [SSL VPN not supported on FortiGate G-series Entry-Level models on page 11](#)
- [SAML certificate verification on page 11](#)

## IPsec phase 1 interface type cannot be changed after it is configured

In FortiOS 7.2.0 and later, the IPsec phase 1 interface type cannot be changed after it is configured. This is due to the tunnel ID parameter (`tun_id`), which is used to match routes to IPsec tunnels to forward traffic. If the IPsec phase 1 interface type needs to be changed, a new interface must be configured.

## FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.2.12 features.

- [FortiGate 6000 incompatibilities and limitations](#)
- [FortiGate 7000E incompatibilities and limitations](#)
- [FortiGate 7000F incompatibilities and limitations](#)



## Hyperscale incompatibilities and limitations

See [Hyperscale firewall incompatibilities and limitations](#) in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.2.12 features.

## SMB drive mapping with ZTNA access proxy

In FortiOS 7.2.5 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

One way to solve the issue is to enter the credentials into Windows Credential Manager in the form of `domain\username`.

Another way to solve the issue is to leverage the KDC proxy to issue a TGT (Kerberos) ticket for the remote user. See [ZTNA access proxy with KDC to access shared drives](#) for more information. This way, there is no reply in Credential Manager anymore, and the user is authenticated against the DC.

## Console error message when FortiGate 40xF boots

In FortiOS 7.2.5 and later, FortiGate 400F and 401F units with BIOS version 06000100 show an error message in the console when booting up.

The message, `Write I2C bus:3 addr:0xe2 reg:0x00 data:0x00 ret:-121.`, is shown in the console, and the FortiGate is unable to get transceiver information.

The issue is fixed in BIOS version 06000101.

## Hyperscale NP7 hardware limitation

Because of an NP7 hardware limitation, for CGN traffic accepted by a hyperscale firewall policy that includes an overload with port block allocation (overload PBA) IP Pool, only one block is allocated per client. The setting of the hyperscale firewall policy `cg-resource-quota` option is ignored.

Because of this limitation, under certain rare conditions (for example, only a single server side IP address and port are being used for a large number of sessions), port allocation may fail even if the block usage of the client is less than its quota. In cases such as this, if the client has traffic towards some other servers or ports,

additional port allocation can become successful. You can also work around this problem by increasing the IP Pool block size (cgn-block-size).

## Changes to NP7 traffic shaping

The following known issues for the Queuing based Traffic Management (QTM) module on NP7 are fixed:

- Incorrect checksum for fragments after QTM.
- Packets longer than 6000 bytes cause QTM to hang.
- Refreshing causes QTM to hang.
- MTU is not honored after QTM, so the packet is not fragmented.

As a result of these changes, you can no longer use the following command to change QoS type used for traffic shaping for sessions offloaded to NP7 processors:

```
config system npu
    set default-qos-type {policing | shaping}
end
```

Instead, default-qos-type can only be set to policing.

For NP7 sessions, policy traffic shaping, per-IP shaping, and regular port shaping (outbandwidth enabled on an interface without a shaping profile) always use the NP7 accounting and traffic shaping module (called the TPE module). This is the same as changing the default-qos-type to policing.

For NP7 sessions, shaping profiles on interfaces now only use QTM for traffic shaping (equivalent to setting default-qos-type to shaping). Shaping profiles on interfaces are also called Multiclass shaping (MCS). The interface can be a physical interface, LAG interface, and VLAN interface (over physical or LAG). The FortiGate supports shaping profiles on a maximum of 100 interfaces.

## GUI cannot be accessed when using a server certificate with an RSA 1024 bit key

The GUI cannot be accessed when using an admin server certificate with an RSA 1024 bit key after upgrading to FortiOS 7.6.1, 7.4.8, or 7.2.11. An RSA key of at least 2048 bits is required. Certificates that are using an RSA key of less than 2048 bits are no longer supported.

## SSL VPN not supported on FortiGate G-series Entry-Level models

The SSL VPN web and tunnel mode feature will not be available from the GUI or the CLI on the FortiGate G-Series Entry-Level models, including 90G and variants. Settings will not be upgraded from previous versions.

Consider migrating to using IPsec Dialup VPN for remote access. See [FortiOS SSL VPN to IPsec VPN migration](#).

## SAML certificate verification

Starting from FortiOS 7.2.12 and 7.6.4, FortiGate verifies the signature for SAML response messages. Please turn on *Sign SAML response and assertion* or similar options in corresponding IDP settings. Lack of signature for signing response messages or assertions may cause authentication to fail.

# Changes in GUI behavior

| Bug ID  | Description  |
|---------|--|
| 1112727 | On a new installation, users logging into the GUI are directed to the FortiCare registration dialog. This ensures that users remember to register their device with FortiCare. This feature is initially supported on FortiGate 900G series and 200G series devices. |

# Changes in default behavior

| Bug ID  | Description   |
|---------|---|
| 985508  | Before the fix, if <code>allow-traffic-redirect</code> enabled (by default), FGT would drop the one arm packet if its source IP is in different subnet from FGT's incoming interface. After the fix, one arm traffic can always pass without policy matching by default.  |
| 1004258 | <p>Add support for <code>cert-probe-failure</code> in <code>firewall ssl-ssh-profile</code> for flow policies. After the upgrade to 7.2.11 or 7.4.5, the setting <code>set cert-probe-failure</code> now applies to flow mode policies. This may result in the following SSL error: <code>SSL connection is blocked due to unable to retrieve the server's certification</code>.</p> <p>To avoid this issue, change the action to allow:</p> <pre>config firewall ssl-ssh-profile     edit "profile_name"         config https             set cert-probe-failure allow         end     end end</pre> |
| 1063233 | The BIOS security level is updated from levels 0/1/2 to levels Low and High. Level High will correspond to previous behaviors in level 2, and level Low will correspond to behaviors in level 1. BIOS that still uses levels 0 will now behave like level 1/Low.  |

# New features or enhancements

More detailed information is available in the [New Features Guide](#).

| Feature ID | Description   |
|------------|---|
| 752946     | <p>To enhance the security of system administrator passwords, FortiGate now uses PBKDF2 as the hashing scheme with randomized salts to hash and store the password.</p> <p>To maintain downgrade support, a new command is introduced:</p> <pre>config system password-policy     set login-lockout-upon-downgrade {enable   disable} end</pre> |
| 1004258    | Add support for cert-probe-failure in firewall ssl-ssh-profile for flow policies.   |
| 1061119    | This enhancement reduces ipshelper CPU usage during the database update process, optimizing system performance and ensuring smoother operations.  |

# Upgrade information

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

Multiple upgrade methods are available for individual FortiGate devices and multiple FortiGate devices in a Fortinet Security Fabric:

| FortiGate  | Upgrade option   | Details  |
|--|--|--|
| Individual FortiGate devices                             | Manual update  | Use the procedure in this topic.<br><br>See also <a href="#">Upgrading individual devices</a> in the FortiOS Administration Guide.                           |
|  | Automatic update based on FortiGuard upgrade path                      | See <a href="#">Enabling automatic firmware updates</a> in the FortiOS Administration Guide for details  |
| Multiple FortiGate devices in a Fortinet Security Fabric | Manual, immediate or scheduled update based on FortiGuard upgrade path | See <a href="#">Fortinet Security Fabric upgrade on page 15</a> and <a href="#">Upgrading Fabric or managed devices</a> in the FortiOS Administration Guide. |

## 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*.

## Fortinet Security Fabric upgrade

FortiOS 7.2.12 greatly increases the interoperability between other Fortinet products. This includes:

|                      |          |
|----------------------|----------|
| <b>FortiAnalyzer</b> | • 7.2.10 |
|----------------------|----------|

|   |   |
|---|---|
| <b>FortiManager</b>                                       | • 7.2.10  |
| <b>FortiExtender</b>                                      | • 7.4.0 and later   |
| <b>FortiSwitch OS<br/>(FortiLink support)</b>             | • 6.4.6 build 0470 or later   |
| <b>FortiAP<br/>FortiAP-S<br/>FortiAP-U<br/>FortiAP-W2</b> | • See <a href="#">Strong cryptographic cipher requirements for FortiAP on page 17</a>                   |
| <b>FortiClient* EMS</b>                                   | • 7.0.3 build 0229 or later   |
| <b>FortiClient* Microsoft<br/>Windows</b>                 | • 7.0.3 build 0193 or later   |
| <b>FortiClient* Mac OS X</b>                              | • 7.0.3 build 0131 or later   |
| <b>FortiClient* Linux</b>                                 | • 7.0.3 build 0137 or later   |
| <b>FortiClient* iOS</b>                                   | • 7.0.2 build 0036 or later   |
| <b>FortiClient* Android</b>                               | • 7.0.2 build 0031 or later   |
| <b>FortiSandbox</b>                                       | • 2.3.3 and later for post-transfer scanning<br>• 4.2.0 and later for post-transfer and inline scanning |

\* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.



When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.2.0, use FortiClient 7.2.0.

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

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



- 14. FortiDeceptor
- 15. FortiAI
- 16. FortiTester
- 17. FortiMonitor
- 18. FortiPolicy



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.12. When Security Fabric is enabled in FortiOS 7.2.12, all FortiGate devices must be running FortiOS 7.2.12.

---

## 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

## Firmware image checksums

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

## Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 and later need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

## FortiGate VM VDOM licenses

FortiGate VMs with one VDOM license (S-series, V-series, FortiFlex) have a maximum number of two VDOMs. An administrative type root VDOM and another traffic type VDOM are allowed in 7.2.0 and later. After upgrading to 7.2.0 and later, if the VM previously had split-task VDOMs enabled, two VDOMs are kept (the root VDOM is an administrative type).

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

Affected versions:

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

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

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

# FortiGate 6000 and 7000 upgrade information

Upgrade FortiGate 6000 firmware from the management board GUI or CLI. Upgrade FortiGate 7000 firmware from the primary FIM GUI or CLI. The FortiGate 6000 management board and FPCs or the FortiGate 7000 FIMs and FPMs all run the same firmware image. Upgrading the firmware copies the firmware image to all components, which then install the new firmware and restart. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

On a standalone FortiGate 6000 or 7000, or an HA cluster with `uninterruptible-upgrade` disabled, the firmware upgrade interrupts traffic because all components upgrade in one step. These firmware upgrades should be done during a quiet time because traffic can be interrupted for a few minutes during the upgrade process.

Fortinet recommends running a graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.



Fortinet recommends that you review the services provided by your FortiGate 6000 or 7000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

## To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.2.12:

1. Use the following command to enable `uninterruptible-upgrade` to support HA graceful upgrade:

```
config system ha
    set uninterruptible-upgrade enable
end
```

2. Download the FortiOS 7.2.12 FG-6000F, FG-7000E, or FG-7000F firmware from <https://support.fortinet.com>.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.  
For example, check the FortiGate dashboard or use the `get system status` command.
5. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

## Upgrade error message

The FortiGate console will print a `Fail to append CC_trailer.ncfg_remove_signature:error in stat error` message after upgrading from 7.2.4 to 7.2.5 or later. Affected platforms include: FFW-3980E, FFW-VM64, and FFW-VM64-KVM. A workaround is to run another upgrade to 7.2.5 or later.

## FortiGates with ULL ports may experience status down on active ports

After upgrading to FortiOS version 7.2.9, FortiGate platforms with ultra-low-latency (ULL) ports like 600F and 901G models may experience link status down on active ULL ports if the following conditions are met:

- The ULL port is set to 25G mode
- Forward error correcting (FEC) is enabled on the port
- Forward error correcting (FEC) is disabled on the connecting switch

This behaviour change is due to a fix in FortiOS 7.2.9 version for an issue where FEC feature was disabled even though it was enabled in the CLI. This allowed the FortiGate ULL port to still connect to the switch with FEC disabled. After the fix, FEC is activated on the FortiGate and caused a mismatch with the switch.

**Workaround:** User can disable FEC feature on the FortiGate ULL port to match with the connecting switch, or they can enable FEC feature on the switch to match with the FortiGate side.

```
config system interface
  edit <ULL port>
    set forward-error-correction disable
  next
end
```

## SLBC FG-5001E primary blade fails to install image

For FG-5001E in a session-aware load balanced cluster (SLBC), all secondary blades install the image successfully. However, the primary blade fails, showing a `sync timeout` error, even with `graceful-upgrade` disabled.

## Admin Access Lockout Risk when upgrading or downgrading from versions with PBKDF2 support

PBKDF2-based password hashing is supported starting in versions 7.2.11, 7.4.8, and 7.6.1. If a device is upgraded to one of these versions and administrator credentials are saved, then later upgraded or downgraded to a release prior to PBKDF2 support (for example, upgrading from 7.2.11 to 7.4.7), the admin login will fail, resulting in administrator access lockout.

Before upgrading or downgrading, make sure that the `login-lockout-upon-downgrade` command is disabled:

```
config system password-policy
    set login-lockout-upon-downgrade disable
end
```

# Product integration and support

The following table lists FortiOS 7.2.12 product integration and support information:

|                                       |   |
|---------------------------------------|---|
| <b>FortiManager and FortiAnalyzer</b> | See the <a href="#">FortiOS Compatibility Tool</a> for information about FortiOS compatibility with FortiManager and FortiAnalyzer.   |
| <b>Web browsers</b>                   | <ul style="list-style-type: none"><li>• Microsoft Edge 114</li><li>• Mozilla Firefox version 113</li><li>• Google Chrome version 114</li></ul> <p>Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.</p>  |
| <b>Explicit web proxy browser</b>     | <ul style="list-style-type: none"><li>• Microsoft Edge 114</li><li>• Mozilla Firefox version 113</li><li>• Google Chrome version 114</li></ul> <p>Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.</p>  |
| <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>Fortinet Single Sign-On (FSSO)</b> | <ul style="list-style-type: none"><li>• 5.0 build 0323 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none"><li>• Windows Server 2022 Standard</li><li>• Windows Server 2022 Datacenter</li><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 64-bit (requires Microsoft SHA2 support package)</li><li>• Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)</li><li>• Windows Server 2008 Core (requires Microsoft SHA2 support package)</li></ul></li><li>• Novell eDirectory 8.8</li></ul> |

|                   |           |
|-------------------|-----------|
| <b>AV Engine</b>  | • 6.00303 |
| <b>IPS Engine</b> | • 7.00363 |

## Virtualization environments

The following table lists hypervisors and recommended versions.

| Hypervisor                      | Recommended versions  |
|---------------------------------|---|
| <b>Citrix Hypervisor</b>        | • 8.1 Express Edition, Dec 17, 2019   |
| <b>Linux KVM</b>                | <ul style="list-style-type: none"> <li>• Ubuntu 18.0.4 LTS</li> <li>• Red Hat Enterprise Linux release 8.4</li> <li>• SUSE Linux Enterprise Server 12 SP3 release 12.3</li> </ul> |
| <b>Microsoft Windows Server</b> | • 2012R2 with Hyper-V role  |
| <b>Windows Hyper-V Server</b>   | • 2019  |
| <b>Open source XenServer</b>    | <ul style="list-style-type: none"> <li>• Version 3.4.3</li> <li>• Version 4.1 and later</li> </ul>  |
| <b>VMware ESXi</b>              | • Versions 6.5, 6.7, 7.0, and 8.0.  |

## Language support

The following table lists language support information.

### Language support

| Language              | GUI |
|-----------------------|-----|
| English               | ✓   |
| Chinese (Simplified)  | ✓   |
| Chinese (Traditional) | ✓   |
| French                | ✓   |
| Japanese              | ✓   |
| Korean                | ✓   |
| Portuguese (Brazil)   | ✓   |
| Spanish               | ✓   |

# SSL VPN support

## SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

### Supported operating systems and web browsers

| Operating System                          | Web Browser   |
|---|---|
| Microsoft Windows 7 SP1 (32-bit & 64-bit) | Mozilla Firefox version 113<br>Google Chrome version 113                            |
| Microsoft Windows 10 (64-bit)             | Microsoft Edge<br>Mozilla Firefox version 113<br>Google Chrome version 113          |
| Ubuntu 20.04 (64-bit)                     | Mozilla Firefox version 113<br>Google Chrome version 113                            |
| macOS Ventura 13                          | Apple Safari version 15<br>Mozilla Firefox version 113<br>Google Chrome version 113 |
| 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.



# Resolved issues

The following issues have been fixed in version 7.2.12. To inquire about a particular bug, please contact [Customer Service & Support](#).

## Firewall

| Bug ID  | Description   |
|---------|---|
| 1117165 | <p>Because of an internal coding change, leaving the apn field of a GTP APN traffic shaping policy empty means the policy will not match any traffic. The intended behavior of an empty apn field is to apply the policy any APN. This type of policy can be useful if the GTP traffic on your network comes from many, possibly unknown, APNs. Currently, you can only apply APN traffic shaping to specific APNs.</p> <p>To configure GTP APN traffic shaping:</p> <pre>config gtp apn-shaper   edit &lt;policy-id&gt;     set apn [&lt;apn-name&gt; &lt;apngrp-name&gt; ...]     set rate-limit &lt;limit&gt;     set action {drop   reject}     set back-off-time &lt;time&gt;   next end</pre> |

## FortiGate 6000 and 7000 platforms

| Bug ID  | Description   |
|---------|---|
| 998615  | When doing a GUI-packet capture on FortiGate, the through-traffic packets are not captured. |
| 1108181 | Unexpected behavior observed in the confsyncd daemon due to an erroneous memory allocation. |
| 1129283 | Bandwidth Widget showing cumulative Tx and Rx rather than current throughput.               |

## FortiSASE

| Bug ID  | Description  |
|---------|--|
| 1140953 | Unable to download large files using HTTPS traffic over internet via SASE. |

## GUI

| Bug ID  | Description   |
|---------|---|
| 1145475 | Multicast traffic dropped when add/remove interface bandwidth widget on dashboard |

## HA

| Bug ID  | Description  |
|---------|--|
| 1117725 | HA synchronization fails due to checksum mismatches on CA certificates across all VDOMs when adding or modifying certificates sourced from a bundle. |
| 1121117 | When two HA clusters are on the same subnet, the L2 session-sync packets could be received by each other even if they are two different HA clusters. |
| 1137565 | vSN support added in 7.2.9, 7.4.6, and 7.6.1. FG-100F/101F do not yet support vSN and logical-sn.  |
| 1138763 | IKE hasync loop and high memory consumption when peer address/port changes   |

## IPsec VPN

| Bug ID  | Description  |
|---------|--|
| 1012615 | After upgrade to 7.4.3 IPsec VPN is dropping traffic   |
| 1059778 | IPsec does not work as expected when the traffic path is from spoke dial-up to hub1, and then from hub1 to another site via a site-to-site tunnel. |

| Bug ID  | Description   |
|---------|---|
| 1110093 | IPSec SA offloading stops on some FortiGate models when handling more than 50,000 concurrent secure associations. |
| 1113354 | Group list got truncated because of fixed size buffers  |
| 1118547 | L2TP over IPSec cannot be established when offloading is enabled on FortiGate-90G .                               |
| 1136536 | VPN authentication fails on FortiSASE when a large number of RADIUS groups are configured.                        |

## Proxy

| Bug ID  | Description  |
|---------|--|
| 877333  | WAD crash with a signal 11 error due to a memory corruption issue when handling VIP cases.   |
| 1135475 | WAD crashes with signal 11 by accessing a null pointer if the client session is close before server connection is done in vs server pool mode. |

## Routing

| Bug ID  | Description   |
|---------|---|
| 1002132 | A BGP neighbor over GRE tunnel does not get established after upgrading due to anti-spoofing not functioning as expected. |

## SSL VPN

| Bug ID  | Description   |
|---------|---|
| 1001272 | The SAML DB Insert does not function as expected and causes a CPU usage issue.  |
| 1026775 | Remove SSL-VPN from FG9xG.  |
| 1122349 | SSL-VPN crashes and disconnects client connections due to a DHCP state machine issue, causing high CPU usage and watchdog timeouts. |

## System

| Bug ID  | Description  |
|---------|--|
| 928743  | Management interface shows up when set status is down.   |
| 986926  | FGT-90xG ULL interface x5, x6, x7, x8 are all down after set to 25G speed.   |
| 1048496 | On FortiGate, the snmp daemon does not work as expected resulting in the SNMP queries timing out.  |
| 1087270 | Unexpected traffic increase over the FortiGate 6000 base backplane.  |
| 1117005 | CPU spikes and management access issues occur on certain FortiGate models post-upgrade when IPsec Phase 1 NPU-offload is enabled during maintenance. |
| 1127534 | Update built-in CRDB bundle to version 1.56.   |
| 1164092 | On NP7 platforms, a change in the destination MAC address or fib change may cause traffic to stop on certain interfaces.                             |

## VM

| Bug ID  | Description   |
|---------|---|
| 1019467 | When the underlying interface is removed, the ipsec tunnel interface will still hold a dst reference. |
| 1092977 | PPPoE interfaces on VM not getting IP address after firmware upgrade.                                 |
| 1157674 | Incorrect system time occurs when FortiGate-VM64-GCP boots up on GCP.                                 |

## Web Filter

| Bug ID                          | Description  |
|---------------------------------|--|
| 1118132,<br>1122036,<br>1127984 | Webfilter local category override not working after reboot in flow mode.   |
| 1131440                         | Webfilter user category override not working after reboot in flow mode.  |
| 1138711                         | Webfilter user category (local and external) override databases are not recreated after Fortigate reboot after reboot or IPS engine restart. |

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 29](#)
- [Existing known issues on page 29](#)

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

## New known issues

There are currently no new issues that have been identified in version 7.2.12.

## FortiGate 6000 and 7000 platforms

| Bug ID  | Description  |
|---------|--|
| 1183735 | Graceful upgrades lead to unintended primary claiming by FortiGate units during HA resynchronization.  |
| 1185528 | Subscription license on the secondary chassis is missing after the graceful upgrade from 7.2.10/11 to 7.2.12.<br><b>Workaround:</b> run <code>execute update-now</code> again. |

## Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.2.12.

### Anti Virus

| Bug ID | Description  |
|--------|--|
| 937375 | Unable to delete malware threat feeds using the CLI. |

## Explicit Proxy

| Bug ID  | Description  |
|---------|--|
| 865828  | Unexpected behavior occurs when configuring internet services with custom or ISDB entries, leading to failed negate options and issues with internet-service6 functionality.   |
| 890776  | The GUI-explicit-proxy setting on the <i>System &gt; Feature Visibility</i> page is not retained after a FortiGate reboot or upgrade.  |
| 894557  | <p>In some cases, the explicit proxy policy list can take a long time to load due to a delay in retrieving the proxy statistics. This issue does not impact explicit proxy functionality.</p> <p><b>Workaround:</b> restart the WAD process, or temporarily disable the WAD debugging process (when FortiGate reboots, this process will need to be disabled again).</p> <p>diagnose wad toggle</p> <p>(use direct connect diagnose)</p> |
| 1059899 | <p>When setting sec-default-action to accept on an initial explicit web proxy configuration after a factory reset, incoming traffic does not match the proxy policy and allows all traffic to pass.</p> <p><b>Workaround:</b> set sec-default-action to deny first in the CLI and then change the setting to accept.</p>   |

## FortiGate 6000 and 7000 platforms

| Bug ID | Description  |
|--------|--|
| 790464 | After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.  |
| 951135 | <p>Graceful upgrade of a FortiGate 6000 or 7000 FGCP HA cluster is not supported when upgrading from FortiOS 7.0.12 to 7.2.6.</p> <p>Upgrading the firmware of a FortiGate 6000 or 7000 FGCP HA cluster from 7.0.12 to 7.2.6 should be done during a maintenance window, since the firmware upgrade process will disrupt traffic for up to 30 minutes.</p> <p>Before upgrading the firmware, disable uninterruptible-upgrade, then perform a normal firmware upgrade. During the upgrade process the FortiGates in the cluster will not allow traffic until all components (management board and FPCs or FIMs and FPMs) are upgraded and both FortiGates have restarted. This process can take up to 30 minutes.</p> |
| 951193 | SLBC for FortiOS 7.0 and 7.2 uses different FGCP HA heartbeat formats. Because of the different heartbeat formats, you cannot create an FGCP HA cluster of two FortiGate 6000s or 7000s when one chassis is running FortiOS 7.0.x and the other is running FortiOS 7.2.x. Instead, to form an FGCP HA cluster, both chassis must be running FortiOS 7.0.x or 7.2.x.  |

| Bug ID  | Description  |
|---------|--|
|         | <p>If two chassis are running different patch releases of FortiOS 7.0 or 7.2 (for example, one chassis is running 7.2.5 and the other 7.2.6), they can form a cluster. When the cluster is formed, FGCP elects one chassis to be the primary chassis. The primary chassis synchronizes its firmware to the secondary chassis. As a result, both chassis will be running the same firmware version.</p> <p>You can also form a cluster if one chassis is running FortiOS 7.2.x and the other is running 7.4.x.</p> <p>For best results, both chassis should be running the same firmware version, although as described above, this is not a requirement.</p>   |
| 954881  | Unintended behavior occurs when FortiGate models perform a warm reboot without properly applying virtual domain configurations.  |
| 994241  | On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.   |
| 1006759 | <p>After an HA failover, there is no IPsec route in the kernel.</p> <p><b>Workaround:</b> Bring down and bring up the tunnel.</p>  |
| 1056894 | On the FortiGate 6000 platform, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.   |
| 1062080 | SNMP query returns an error when there is a large number of BGP routes.  |
| 1070365 | <p>FGCP HA session synchronization may stop working as expected on a FortiGate 7000F cluster managed by FortiManager. This happens if the HA configuration uses management interfaces as session synchronization interfaces by configuring the session-sync-dev option, for example:</p> <pre>config system ha     set session-sync-dev 1-M1 1-M2 end</pre> <p>The problem occurs when FortiManager updates the configuration of the FortiGate 7000F devices in the cluster it incorrectly changes to the VDOM of the management interfaces added to the session-sync-dev command from mgmt-vdom to vsys_ha and the interfaces stop working as session sync interfaces.</p> <p>You can work around the problem by manually changing the vdom of the management interfaces added to session-sync-dev to mgmt-vdom and then retrieving the FortiGate configuration from FortiManager.</p> <pre>config system interface     edit 1-M1         set vdom mgmt-vdom     next     edit 1-M2         set vdom mgmt-vdom     next end</pre> |

| Bug ID  | Description  |
|---------|--|
| 1093412 | For an FGSP configuration on the FortiGate 6000 and 7000 platforms, the encryption option of the <code>config system standalone-cluster</code> command does not encrypt session synchronization traffic. Enabling this option has no effect. |
| 1096156 | GUI unreachable due to certificates and private keys mismatch in a HA setup.   |
| 1149342 | BGP flapping occurs when concurrent IP address management causes unexpected source IP usage on outbound connections during FortiGate VDOM migrations.  |

## FortiView


| Bug ID  | Description  |
|---------|--|
| 1123502 | FortiView Threats: drilling down to malicious website entry returns <i>Failed to retrieve FortiView data from disk</i> . |

## GUI

| Bug ID  | Description   |
|---------|---|
| 853352  | On the <i>View/Edit Entries</i> slide-out pane ( <i>Policy &amp; Objects &gt; Internet Service Database</i> dialog), users cannot scroll down to the end if there are over 100000 entries.  |
| 974988  | FortiGate GUI should not display a license expired notification due to an expired FortiManager Cloud license if it still has a valid account level FortiManager Cloud license (function is not affected).   |
| 989512  | When the number of users in the <i>Firewall User</i> monitor exceeds 2000, the search bar, column filters, and graphs are no longer displayed due to results being lazily loaded.   |
| 993890  | The Node.JS daemon restarts with a <code>kill ESRCH</code> error on FortiGate after an upgrade.   |
| 999972  | Edits that are made to <i>IP Exemptions</i> in <i>IPS Signatures and Filters</i> more than once on the <i>Security Profiles &gt; Intrusion Prevention</i> page are not saved.   |
| 1055197 | On FortiGate G series models with dual WAN links, the <i>Interface Bandwidth</i> widget may show an incorrect incoming and outgoing bandwidth count where the actual traffic does not match the display numbers.  |
| 1143734 | Network > SD-WAN > SD-WAN Rules: When editing a rule, inline edit from the omniselect is not available for Application Group entries.<br><b>Workaround:</b> edit the application from Security Profiles > Application Signatures > Group or using the command line. |



## HA

| Bug ID  | Description   |
|---------|---|
| 781171  | <p>When performing HA upgrade in the GUI, if the secondary unit takes several minutes to bootup, the GUI may show a misleading error message <i>Image upgrade failed</i> due to premature timeout.</p> <p>This is just a GUI display issue and the HA upgrade can still complete without issue.</p>   |
| 970316  | <p>When adding a new vcluster, the link-failure value of the newly added vcluster is not updated, causing the wrong primary unit to be selected.</p>  |
| 988944  | <p>The Fabric Management page displays inconsistent information when accessed through secondary HA units on some FortiGate models.</p>  |
| 1072440 | <p>Special branch supported models of FortiGate in an HA cluster with an empty HA password, upgrading from a special build GA version (version 7.0.x) to version 7.2.9 and version 7.2.10 GA can cause one of the members to not upgrade.</p> <p>Impacted models: Please see a full list of <a href="#">Special branch supported models</a> for FortiOS version 7.0.15.</p> <p><b>Workaround:</b> configure a valid HA password for the cluster before the upgrade, or manually upgrade the member that was impacted.</p> <pre>config system ha     set password &lt;new-password&gt; end</pre> <hr/> <div>  <p>Setting the password causes an HA cluster re-election to occur.</p> </div> |

## Hyperscale

| Bug ID | Description   |
|--------|---|
| 802182 | <p>After successfully changing the VLAN ID of an interface from the CLI, an error message similar to <code>cmdb_txn_cache_data(query=log.npu-server,leve=1)</code> failed may appear.</p> |
| 817562 | <p>LPMD fails to correctly handle different VRFs, treating all as vrf 0, causing improper route management and affecting network traffic isolation.</p>                                   |
| 824071 | <p>IPv6 traffic fails to load balance across multiple virtual domains when using Equal-cost Multipath (ECMP) in NAT mode on FortiGate devices.</p>  |
| 843197 | <p>The npu-session list fails to display policy-route information when traffic is routed through a policy route on FortiGate models using NPU acceleration.</p>                           |
| 853258 | <p>Traffic drops occur after Failover in HA A-P setups using hardware-only sessions.</p>  |

| Bug ID  | Description  |
|---------|--|
| 872146  | The "diagnose sys npu-session list" command displays incorrect policy IDs when traffic uses intra-zone policies.                           |
| 920228  | NAT46 NPU sessions are lost and traffic drops when a HA failover occurs.   |
| 1170648 | <code>diagnose firewall ippool list pba</code> command is executed in a hyperscale device may result in high CPU. No workaround available. |

## IPsec VPN

| Bug ID  | Description   |
|---------|---|
| 944600  | CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.  |
| 1128662 | BGP peering fails to establish when a race condition occurs between FortiGate OS and NPU driver during IPsec SA updates for dynamic hub-to-static spoke VPNs. |

## Proxy

| Bug ID | Description   |
|--------|---|
| 910678 | CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature. |

## REST API

| Bug ID  | Description  |
|---------|--|
| 1004136 | Unable to fetch more than 1000 logs using an REST API GET request. |

## Routing

| Bug ID | Description  |
|--------|--|
| 896090 | SD-WAN Performance SLA health checks fail when FortiGuard is configured as the server due to lack of HTTP support on FortiGuard servers. |
| 903444 | The <code>diagnose ip rtcache list</code> command is no longer supported in the FortiOS 4.19 kernel.                                     |

| Bug ID  | Description  |
|---------|--|
| 912070  | The client learned the physical MAC address of the FortiGate secondary instead of the VR MAC when requesting the VIP, despite the primary FortiGate sending the initial ARP response.                      |
| 924693  | On the <i>Network &gt; SD-WAN &gt; SD-WAN Rules</i> page, member interfaces that are down are incorrectly shown as up. The tooltip on the interface shows the correct status.                              |
| 1025201 | FortiGate encounters a duplication issue in a hub and spoke configuration with <code>set packet-duplication force</code> enabled on a spoke and <code>set packet-de-duplication</code> enabled on the hub. |

## Security Fabric

| Bug ID  | Description   |
|---------|---|
| 903922  | Security Fabric physical and logical topology is slow to load when there are a lot of downstream devices, including FortiGates, FortiSwitches, FortiAPs, and endpoint device traffic. This is a GUI only display issue and does not impact operations of downstream devices.  |
| 1011833 | FortiGate experiences a CPU usage issue in the node process when there multiple administrator sessions running simultaneously on the GUI in a Security Fabric with multiple downstream devices. This may result in slow loading times for multiple GUI pages.<br><b>Workaround:</b> disconnect the other concurrent administrator sessions to avoid overloading node process. |
| 1120652 | Fabric topology with two devices on different VDOMs but behind the same router shows wrong VDOM data on tooltip.<br><b>Workaround:</b> Disable device-identification on that interface.   |

## SSL VPN

| Bug ID | Description   |
|--------|---|
| 795381 | FortiClient Windows cannot be launched with SSL VPN web portal.   |
| 941676 | Incorrect character entered when using Shift+2 on Japanese keyboard during RDP session in SSL-VPN web mode. |

## Switch Controller

| Bug ID | Description   |
|--------|---|
| 947351 | The FortiSwitch topology fails to load correctly and triggers Java errors in HTTPS logs when switches are connected via SFPs. |
| 961142 | An interface in FortiLink is flapping with MCLAG with DAC on an OPSFPP-T-05-PAB transceiver.                                  |

## System

| Bug ID  | Description   |
|---------|---|
| 782710  | VLAN-over-VXLAN traffic was not being offloaded to NP7, causing performance issues due to increased CPU load.   |
| 882862  | On FortiGate 400F, 600F, 900G, 3200F, and 3700F models, LAG interface members are not shutting down when the remote end interface (one member in the LAG) is admin down.  |
| 901621  | <p>On the NP7 platform, setting the interface configuration using set inbandwidth &lt;x&gt; or set outbandwidth &lt;x&gt; commands stops traffic flow.</p> <p><b>Workaround:</b> Change the NP7 ""default-qos-type"" setting from shaping to policing. This requires a restart of the device for the configuration to take effect.</p> <pre>config system npu     set default-qos-type policing end</pre> |
| 921604  | On the FortiGate 601F, the ports (x7) have no cables attached but the link LEDs are green.  |
| 1045866 | The node daemon causes a CPU usage and memory usage issue when many interfaces are being edited or created at once.   |
| 1078119 | Traffic is intermittently interrupted on virtual-vlan-switch on Soc5 based platforms when a multicast or broadcast packet is received.  |
| 1078541 | <p>The FortiFirewall 2600F model may become stuck after a fresh image burn. Upgrading from a previous version stills works.</p> <p><b>Workaround:</b> power cycle the unit.</p>   |
| 1114594 | <p>On the FG-200G, SDNS is not able to connect to FortiGuard servers.</p> <p><b>Workaround:</b> use DNS instead of SDNS.</p> <pre>config system dns     set protocol cleartext end</pre>  |
| 1117005 | <p>FortiGate encounters a CPU usage issue.</p> <p><b>Workaround:</b> Disable IPsec phase1 npu-offload.</p>  |

| Bug ID  | Description   |
|---------|---|
| 1121548 | Enabling device-identification also gets endpoint information, even though intermediate router exists on FG and endpoints.<br><b>Workaround:</b> Disable device-identification on that interface. |

## Upgrade

| Bug ID  | Description   |
|---------|---|
| 1055486 | On the <i>Firmware and Registration</i> page, when performing a Fabric Upgrade using the GUI for the whole Fabric topology that includes managed FortiAPs and FortiSwitches, the root FortiGate may use an incorrect recommended image for FortiAP and FortiSwitch due to a parsing issue.<br><b>Workaround:</b> initiate the Fabric Upgrade using the CLI. |

## User & Authentication

| Bug ID  | Description   |
|---------|---|
| 1043189 | Low-end FortiGate models with 2GB memory may enter conserve mode when processing large user store data with over 5000 user records and each record has a large number of IoT vulnerability data.<br>For example, the <i>Users and Devices</i> page or FortiNAC request can trigger the following API call that causes the httpsd process encounter a CPU usage issue and memory usage issue.<br><br>GET request /api/v2/monitor/user/device/query |

## VM

| Bug ID  | Description   |
|---------|---|
| 899984  | If FGTVM was deployed in UEFI boot mode, do not downgrade to any GA version earlier than 7.2.4.                                 |
| 1094274 | FortiOS becomes unresponsive when sending IPv6 traffic over MLX5 network adapters due to incorrect WQE handling.                |
| 1119140 | Incorrect deployment of DLP configurations occurs when FortiGate VMs are deployed on hypervisors with Intel Skylake processors. |

## Web Filter

| Bug ID | Description  |
|--------|--|
| 885222 | HTTP sessions are logged as HTTPS in web filter logs when using an HTTP VIP server, causing incorrect protocol identification. |

## WiFi Controller

| Bug ID | Description   |
|--------|---|
| 869106 | The layer 3 roaming feature may not work when the wireless controller is running multiple cw_acd processes (when the value of acd-process-count is not zero). |
| 869978 | In HA cluster of FGT-200F units with 'capwap-offload' enabled, traffic from tunnel SSID cannot pass after HA failover is triggered.                           |
| 873273 | The automatically connect option fails to function when the local radio connection is lost on some FortiGate models.  |
| 941691 | Managed FortiSwitch detects multiple MACs using the same IP address.  |

## ZTNA

| Bug ID | Description   |
|--------|---|
| 819987 | Mapped drives become inaccessible after laptop reboots when using FortiGate ZTNA access proxy with FQDN destinations. |

# Built-in AV Engine

AV Engine 6.00303 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

# Built-in IPS Engine

IPS Engine 7.00363 is released as the built-in IPS Engine.



# 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.

## Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models

FortiGate Rugged 60F and 60F 3G4G models have various generations defined as follows:

- Gen1
- Gen2 = Gen1 + TPM
- Gen3 = Gen2 + Dual DC-input
- Gen4 = Gen3 + GPS antenna
- Gen5 = Gen4 + memory

The following HA clusters can be formed:

- Gen1 and Gen2 can form an HA cluster.
- Gen4 and Gen5 can form an HA cluster.

- Gen1 and Gen2 cannot form an HA cluster with Gen3, Gen4, or Gen5 due to differences in the `config system vin-alarm` command.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.