

# Release Notes

**FortiOS 7.2.10**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



September 20, 2024

FortiOS 7.2.10 Release Notes

01-7210-1073605-20240920

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>Introduction and supported models</b>	<b>7</b>
Supported models	7
FortiGate 6000 and 7000 support	7
<b>Special notices</b>	<b>9</b>
IPsec phase 1 interface type cannot be changed after it is configured	9
IP pools and VIPs are now considered local addresses	9
FortiGate 6000 and 7000 incompatibilities and limitations	10
Hyperscale incompatibilities and limitations	10
SMB drive mapping with ZTNA access proxy	10
Console error message when FortiGate 40xF boots	10
FortiGate models with 2 GB RAM cannot be a Security Fabric root	10
FortiGuard Web Filtering Category v10 update	11
FortiAP-W2 models may experience bootup failure during federated upgrade process if they are powered by a managed FortiSwitch's PoE port	12
Remote access with write rights through FortiGate Cloud	12
Hyperscale NP7 hardware limitation	12
RADIUS vulnerability	12
<b>Changes in CLI</b>	<b>14</b>
<b>Changes in GUI behavior</b>	<b>15</b>
<b>Changes in default behavior</b>	<b>16</b>
<b>Changes in table size</b>	<b>17</b>
<b>New features or enhancements</b>	<b>18</b>
<b>Upgrade information</b>	<b>20</b>
Fortinet Security Fabric upgrade	20
Downgrading to previous firmware versions	22
Firmware image checksums	22
Strong cryptographic cipher requirements for FortiAP	22
FortiGate VM VDOM licenses	23
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name	23
FortiGate 6000 and 7000 upgrade information	23
IPS-based and voipd-based VoIP profiles	24
Upgrade error message	25
BIOS-level signature and file integrity checking during downgrade	25
FortiOS restricts the automatic firmware upgrades to the FortiGate	26
GUI firmware upgrade does not follow the recommended upgrade path in previous versions	27
Upgrading from 7.2.4 or earlier versions	27
FortiGates with ULL ports may experience status down on active ports	27

<b>Product integration and support</b>	<b>29</b>
Virtualization environments	30
Language support	30
SSL VPN support	31
SSL VPN web mode	31
<b>Resolved issues</b>	<b>32</b>
Proxy	32
SSL VPN	32
Switch Controller	32
VM	32
<b>Known issues</b>	<b>33</b>
New known issues	33
Explicit Proxy	33
Firewall	33
FortiGate 6000 and 7000 platforms	33
GUI	34
HA	34
Intrusion Prevention	34
Routing	34
System	34
User & Authentication	35
Existing known issues	35
Anti Virus	35
Explicit Proxy	35
Firewall	36
FortiGate 6000 and 7000 platforms	36
GUI	37
HA	38
Hyperscale	38
IPsec VPN	39
Log & Report	39
Proxy	39
REST API	39
Routing	39
Security Fabric	40
SSL VPN	40
Switch Controller	40
System	40
Upgrade	41
User & Authentication	41
VM	42
Web Filter	42
WiFi Controller	42
ZTNA	42

---

<b>Built-in AV Engine</b> .....	<b>43</b>
<b>Built-in IPS Engine</b> .....	<b>44</b>
<b>Limitations</b> .....	<b>45</b>
Citrix XenServer limitations .....	45
Open source XenServer limitations .....	45

# Change Log

Date	Change Description
2024-09-19	Initial release.
2024-09-20	Updated <a href="#">RADIUS vulnerability on page 12</a> and <a href="#">Known issues on page 33</a> .

# Introduction and supported models

This guide provides release information for FortiOS 7.2.10 build 1706.

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

## Supported models

FortiOS 7.2.10 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

## FortiGate 6000 and 7000 support

FortiOS 7.2.10 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 9
- IP pools and VIPs are now considered local addresses on page 9
- FortiGate 6000 and 7000 incompatibilities and limitations on page 10
- Hyperscale incompatibilities and limitations on page 10
- SMB drive mapping with ZTNA access proxy on page 10
- Console error message when FortiGate 40xF boots on page 10
- FortiGate models with 2 GB RAM cannot be a Security Fabric root on page 10
- FortiGuard Web Filtering Category v10 update on page 11
- FortiAP-W2 models may experience bootup failure during federated upgrade process if they are powered by a managed FortiSwitch's PoE port on page 12
- Remote access with write rights through FortiGate Cloud on page 12
- Hyperscale NP7 hardware limitation on page 12
- RADIUS vulnerability on page 12

## 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.

## IP pools and VIPs are now considered local addresses

In FortiOS 7.2.6 and later, all IP addresses used as IP pools and VIPs are now considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is considered a destination for those IP addresses and can receive reply traffic at the application layer.

Previously in FortiOS 7.2.0 to 7.2.5, this was not the case. For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see [Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4](#).

## FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.2.10 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 7.2.10 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.

## FortiGate models with 2 GB RAM cannot be a Security Fabric root

A Security Fabric topology is a tree topology consisting of a FortiGate root device and downstream devices within the mid-tier part of the tree or downstream (leaf) devices at the lowest point of the tree.

As part of improvements to reducing memory usage on FortiGate models with 2 GB RAM, this version of FortiOS no longer allows these models to be the root of the Security Fabric topology or any mid-tier part of the topology. Therefore, FortiGate models with 2 GB RAM can only be a downstream device in a Security Fabric or a standalone device.

The affected models are the FortiGate 40F, 60E, 60F, 80E, and 90E series devices and their variants.



FortiGate models with 2 GB RAM running FortiOS 7.4.2 or later can be used as the Security Fabric root. See [FortiGate models with 2 GB RAM can be a Security Fabric root](#).

---

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

In the GUI on the *Security Fabric > Fabric Connectors* page when editing the *Security Fabric Setup* card, the *Security Fabric role* can only be configured as *Standalone* or *Join Existing Fabric*.

In the CLI, the following error messages are displayed when attempting to configure a FortiGate model with 2 GB RAM as a Security Fabric root:

```
config system csf
    set status enable
end
```

...

```
2GB-RAM models cannot be a Security Fabric root.
Please set the upstream.
object set operator error, -39, roll back the setting
Command fail. Return code -39
```

## FortiGuard Web Filtering Category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the versions below:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:

<https://support.fortinet.com/Information/Bulletin.aspx>

## FortiAP-W2 models may experience bootup failure during federated upgrade process if they are powered by a managed FortiSwitch's PoE port

Disable the federated upgrade feature if you have FortiAP-W2 devices that are exclusively powered by a PoE port from a FortiGate or FortiSwitch.

The federated upgrade feature starts the upgrades of managed FortiSwitch and FortiAP devices at approximately the same time. Some FortiAP-W2 devices take a longer time to upgrade than the FortiSwitch devices. When the FortiSwitch finishes upgrading, it reboots, and can disrupt the PoE power to the FortiAP devices. If a FortiAP device is still upgrading when the power is disrupted, it can cause the FortiAP device to experience a bootup failure.

Manually triggering federated upgrade can cause this issue. Starting in 7.2.8, automatic firmware upgrade will no longer trigger FortiSwitch and FortiAP to be upgraded.

For more information about federated upgrade, see [Upgrading Fabric or managed devices](#).

## Remote access with write rights through FortiGate Cloud

Remote access with read and write rights through FortiGate Cloud now requires a paid FortiGate Cloud subscription. The FortiGate can still be accessed in a read-only state with the free tier of FortiGate Cloud. Alternatively, you can access your FortiGate through its web interface.

Please contact your Fortinet Sales/Partner for details on purchasing a FortiGate Cloud Service subscription license for your FortiGate device.

For more information see the [FortiGate Cloud feature comparison](#) and [FortiGate Cloud Administration guide FAQ](#).

## 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 (`cg-block-size`).

## RADIUS vulnerability

Fortinet has resolved a RADIUS vulnerability as described in CVE-2024-3596. As a result, firewall authentication, FortiGate administrative web UI authentication, and WiFi authentication may be affected depending on the functionality

of the RADIUS server software used in your environment. RFC 3579 contains information on the affected RADIUS attribute, message-authenticator.

In order to protect against the RADIUS vulnerability described in CVE-2024-3596, as a RADIUS client, FortiGate will:

1. Force the validation of message-authenticator.
2. Reject RADIUS responses with unrecognized proxy-state attribute.

Message-authenticator checking is made mandatory under UDP/TCP. It is not mandatory when using TLS. Users are highly encouraged to use RADSEC with the RADIUS server configuration, which is supported starting in version 7.4.0. For more information, see [Configuring a RADSEC client](#).

If FortiGate is using UDP/TCP mode without RADSEC, the RADIUS server should be patched to ensure the message-authenticator attribute is used in its RADIUS messages.

### **Affected Product Integration**

- FortiAuthenticator version 6.6.1 and older.

### **Solution**

- Upgrade FortiAuthenticator to version 6.6.2 and follow the [Upgrade instructions](#).

## Changes in CLI

Bug ID	Description
913040	<p>The <code>config vpn ssl settings option tunnel-addr-assigned-method</code> is now available again in the FortiGate 6000 and 7000 CLI. This option had been removed in a previous release because setting this option to <code>first-available</code> and configuring multiple IP pools was found to reduce FortiGate 6000 and 7000 SSL VPN load balancing performance. However, some users may want the ability to use multiple IP pools for their SSL VPN configuration, even if performance is reduced. So the change has been reverted.</p>
921914	<p>The URL to verify authentication has been removed from <code>config user saml</code> and replaced by <code>config user external-identity provider</code>.</p> <p><b>7.2.7 and earlier:</b></p> <pre>config user saml   edit &lt;name&gt;     set auth-url &lt;string&gt;   next end</pre> <p><b>7.2.8 and later:</b></p> <pre>config user external-identity-provider   edit &lt;name&gt;     set type ms-graph     set version v1.0   next end</pre> <p>After the external identity provider is set, make sure that the existing user group has both the SAML server and the external identity provider as members:</p> <pre>config user group   edit &lt;group&gt;     set member &lt;saml server&gt; &lt;id provider&gt;   next end</pre>

## Changes in GUI behavior

Bug ID	Description
1043593	On the <i>Network &gt; Diagnostics &gt; Packet Capture</i> page, the timeline graph is removed from the packet viewer.

## Changes in default behavior

Bug ID	Description
1006011	Starting with version 7.4.4, FMG-Access is no longer enabled by default on all interfaces. In the event of an upgrade from a previous version, if the central-management type is not set as FortiManager, the fgfm will be disabled across all interfaces.




## Changes in table size

Bug ID	Description
823373	Increase the number of VRFs per VDOM from 64 to 252.

# New features or enhancements

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

Feature ID	Description
913213	When authenticating users with a RADIUS server, FortiOS can now dynamically assign a different NAS-IP-Address attribute to the managed switches. For more control, this feature also allows you to manually override the dynamic assignment and set the NAS-IP-Address attribute for individual switches as per your requirements.
936747	<p>On FortiGates with multiple NP7 processors with hyperscale enabled, you can use the following command to optimize NP7 network session setup (NSS) engine performance.</p> <pre>config system npu     set nss-threads-option {4T-EIF   4T-NOEIF   2T} end</pre> <ul style="list-style-type: none"><li>• <b>4T-EIF</b>: the NSS is configured with four threads and the Endpoint Independent Filtering (EIF) feature is allowed (the default). NSS with four threads supports the maximum NP7 Connections Per Second (CPS) performance.</li><li>• <b>4T-NOEIF</b>: the NSS is configured with four threads and the EIF feature is not allowed. Also supports the maximum NP7 CPS performance.</li><li>• <b>2T</b>: the NSS is configured with two threads and the EIF feature is allowed. This setting reduces the maximum NP7 CPS performance.</li></ul> <hr/> <div> Changing the <code>nss-threads-option</code> causes the FortiGate to restart.</div> <hr/>
955835	Previously, when auto-upgrade was disabled, users would receive a warning advising them to execute <code>exec federated-upgrade cancel</code> in order to remove any scheduled upgrades. However, with the new update, the system is now capable of autonomously canceling any pending upgrades, eliminating the need for manual user action.
973573	You can now specify a tagged VLAN for users to be assigned to when the authentication server is unavailable. Previously, you could only specify an untagged VLAN. This feature is available with 802.1x MAC-based authentication. It is compatible with both Extensible Authentication Protocol (EAP) and MAC authentication bypass (MAB).
1006448	Enhance SSL VPN security by restricting and validating HTTP messages that are used only by web mode and tunnel mode.
1007937	Support the Zstandard (zstd) compression algorithm for web content. This enhancement enables FortiOS to decode, scan, and forward zstd-encoded web content in a proxy-based policy. The content can then be passed or blocked based on the UTM profile settings. This ensures a seamless and secure browsing experience.

Feature ID	Description
1012626	In this enhancement, a hash of all executable binary files and shared libraries are taken during image build time. The file containing these hashes, called the executable hash, is also hashed and as a result signed. The signature for this hash is verified during bootup to ensure integrity of the file. After validation, the hashes of all executable and share libraries can be loaded into memory for real-time protection.
1013511	This enhancement requires the kernel to verify the signed hashes of important file-system and object files during boot-up. This prevents unauthorized changes to file-systems to be mounted, and other unauthorized objects to be loaded into user space on boot-up. If the signed hash verification fails, the system will halt.

# 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.  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 20</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 7.2.10 greatly increases the interoperability between other Fortinet products. This includes:

<b>FortiAnalyzer</b>	• 7.2.7
<b>FortiManager</b>	• 7.2.7
<b>FortiExtender</b>	• 7.4.0 and later

<b>FortiSwitch OS (FortiLink support)</b>	<ul style="list-style-type: none"> <li>• 6.4.6 build 0470 or later</li> </ul>
<b>FortiAP FortiAP-S FortiAP-U FortiAP-W2</b>	<ul style="list-style-type: none"> <li>• See <a href="#">Strong cryptographic cipher requirements for FortiAP on page 22</a></li> </ul>
<b>FortiClient* EMS</b>	<ul style="list-style-type: none"> <li>• 7.0.3 build 0229 or later</li> </ul>
<b>FortiClient* Microsoft Windows</b>	<ul style="list-style-type: none"> <li>• 7.0.3 build 0193 or later</li> </ul>
<b>FortiClient* Mac OS X</b>	<ul style="list-style-type: none"> <li>• 7.0.3 build 0131 or later</li> </ul>
<b>FortiClient* Linux</b>	<ul style="list-style-type: none"> <li>• 7.0.3 build 0137 or later</li> </ul>
<b>FortiClient* iOS</b>	<ul style="list-style-type: none"> <li>• 7.0.2 build 0036 or later</li> </ul>
<b>FortiClient* Android</b>	<ul style="list-style-type: none"> <li>• 7.0.2 build 0031 or later</li> </ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"> <li>• 2.3.3 and later for post-transfer scanning</li> <li>• 4.2.0 and later for post-transfer and inline scanning</li> </ul>

\* 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 7.2.10. When Security Fabric is enabled in FortiOS 7.2.10, all FortiGate devices must be running FortiOS 7.2.10.

---

## 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 7.2.10:

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 7.2.10 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.

## IPS-based and voipd-based VoIP profiles

Starting in FortiOS 7.2.5, the new IPS-based VoIP profile allows flow-based SIP to complement SIP ALG while working together. There are now two types of VoIP profiles that can be configured:

```
config voip profile
    edit <name>
        set feature-set {ips | voipd}
    next
end
```

A voipd-based VoIP profile is handled by the voipd daemon using SIP ALG inspection. This is renamed from proxy in previous FortiOS versions.

An ips-based VoIP profile is handled by the IPS daemon using flow-based SIP inspection. This is renamed from flow in previous FortiOS versions.

Both VoIP profile types can be configured at the same time on a firewall policy. For example:

```
config firewall policy
    edit 1
        set voip-profile "voip_sip_alg"
        set ips-voip-filter "voip_sip_ips"
    next
end
```

Where:



- `voip-profile` can select a `voip-profile` with `feature-set voipd`.
- `ips-voip-filter` can select a `voip-profile` with `feature-set ips`.

The VoIP profile selection within a firewall policy is restored to pre-7.0 behavior. The VoIP profile can be selected regardless of the inspection mode used in the firewall policy. The new `ips-voip-filter` setting allows users to select an IPS-based VoIP profile to apply flow-based SIP inspection, which can work concurrently with SIP ALG.

Upon upgrade, the `feature-set` setting of the `voip` profile determines whether the profile applied in the firewall policy is `voip-profile` or `ips-voip-filter`.

Before upgrade	After upgrade
<pre> config voip profile   edit "ips_voip_filter"     set feature-set flow   next   edit "sip_alg_profile"     set feature-set proxy   next end </pre>	<pre> config voip profile   edit "ips_voip_filter"     set feature-set ips   next   edit "sip_alg_profile"     set feature-set voipd   next end </pre>
<pre> config firewall policy   edit 1     set voip-profile "ips_voip_filter"   next   edit 2     set voip-profile "sip_alg_profile"   next end </pre>	<pre> config firewall policy   edit 1     set ips-voip-filter "ips_voip_ filter"   next   edit 2     set voip-profile "sip_alg_profile"   next end </pre>

## 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.

## BIOS-level signature and file integrity checking during downgrade

When downgrading to a version of FortiOS prior to 6.4.13, 7.0.12, and 7.2.5 that does not support BIOS-level signature and file integrity check during bootup, the following steps should be taken if the BIOS version of the FortiGate matches the following versions:

- 6000100 or greater
- 5000100 or greater

**To downgrade or upgrade to or from a version that does not support BIOS-level signature and file integrity check during bootup:**

1. If the current security level is 2, change the security level to 0. This issue does not affect security level 1 or below.
2. Downgrade to the desired FortiOS firmware version.
3. If upgrading back to 6.4.13, 7.0.12, 7.2.5, 7.4.0, or later, ensure that the security level is set to 0.
4. Upgrade to the desired FortiOS firmware version.
5. Change the security level back to 2.

**To verify the BIOS version:**

The BIOS version is displayed during bootup:

```
Please stand by while rebooting the system.  
Restarting system  
FortiGate-1001F (13:13-05.16.2023)  
Ver: 06000100
```

**To verify the security level:**

```
# get system status  
Version: FortiGate-VM64 v7.4.2,build2571,231219 (GA.F)  
First GA patch build date: 230509  
Security Level: 1
```

**To change the security level:**

1. Connect to the console port of the FortiGate.
2. Reboot the FortiGate (`execute reboot`) and enter the BIOS menu.
3. Press [I] to enter the *System Information* menu
4. Press [U] to enter the *Set security level* menu
5. Enter the required security level.
6. Continue to boot the device.

## FortiOS restricts the automatic firmware upgrades to the FortiGate

Automatic firmware upgrades update the FortiGate and any connected FortiSwitch, FortiAP, and FortiExtender devices. This caused issues with FortiAPs going into a boot loop due to reboot timing. Starting from FortiOS 7.2.8, a temporary fix is introduced: restrict the automatic firmware upgrades to the FortiGate only.

## GUI firmware upgrade does not follow the recommended upgrade path in previous versions

When performing a firmware upgrade from 7.2.0 - 7.2.8 that requires multiple version jumps, the *Follow upgrade path* option in the GUI does not respect the recommended upgrade path, and instead upgrades the firmware directly to the final version. This can result in unexpected configuration loss. To upgrade a device in the GUI, upgrade to each interim version in the upgrade path individually.

For example, when upgrading from 7.0.7 to 7.0.12 the recommended upgrade path is 7.0.7 -> 7.0.9 -> 7.0.11 -> 7.0.12. To ensure that there is no configuration loss, first upgrade to 7.0.9, then 7.0.11, and then 7.0.12.

## Upgrading from 7.2.4 or earlier versions

If your device is running on version 7.2.4 or earlier, you must upgrade the device to version 7.2.5, 7.2.6, 7.2.7 or 7.2.8 first by following recommended upgrade path before upgrading to version 7.2.9. A direct upgrade from 7.2.4 or below to 7.2.9 will cause the system bootup to hang.

Similarly, upgrading from 7.0.11 or below directly to 7.2.9 is not supported. Please follow the recommended upgrade path before upgrading to version 7.2.9.

If upgrading from the GUI, upgrade to each firmware version in the upgrade path individually. Do not use the *Follow upgrade path* option.

In the event of the system hanging due to the upgrade process to version 7.2.9, boot up from a backup partition using BIOS, then continue the upgrade by following the upgrade path.

Find your upgrade path from the [Upgrade Path Tool](#).

## 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
```

# Product integration and support

The following table lists FortiOS 7.2.10 product integration and support information:

<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 0318 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><li>• Novell eDirectory 8.8</li></ul></li></ul>
<b>AV Engine</b>	<ul style="list-style-type: none"><li>• 6.00301</li></ul>
<b>IPS Engine</b>	<ul style="list-style-type: none"><li>• 7.00342</li></ul>

## Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
<b>Citrix Hypervisor</b>	<ul style="list-style-type: none"> <li>8.1 Express Edition, Dec 17, 2019</li> </ul>
<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>	<ul style="list-style-type: none"> <li>2012R2 with Hyper-V role</li> </ul>
<b>Windows Hyper-V Server</b>	<ul style="list-style-type: none"> <li>2019</li> </ul>
<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>	<ul style="list-style-type: none"> <li>Versions 6.5, 6.7, 7.0, and 8.0.</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 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 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Ventura 13	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

## Resolved issues

The following issues have been fixed in version 7.2.10. To inquire about a particular bug, please contact [Customer Service & Support](#).

### Proxy

Bug ID	Description
912116	Website (li***.cz) is not working in proxy inspection mode with deep inspection and web filter applied.

### SSL VPN

Bug ID	Description
893190	FortiGate does not utilize timeout timers correctly for 2FA when SSL VPN is used as a server.
983513	The <code>two-factor-fac-expiry</code> command is not working as expected for remote RADIUS users with a remote token set in FortiAuthenticator.
1061165	SSL VPN encounters a signal 11 interruption and does not work as expected due to a word-length heap memory issue.

### Switch Controller

Bug ID	Description
1032105	FortiGate in an HA configuration goes out of synchronization due to a split-port interface on FortiSwitch.

### VM

Bug ID	Description
1073016	The OCI SDN connector cannot call the API to the Oracle service when an IAM role is enabled.



# Known issues

Known issues are organized into the following categories:

- [New known issues on page 33](#)
- [Existing known issues on page 35](#)

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

## New known issues

The following issues have been identified in version 7.2.10.

### Explicit Proxy

Bug ID	Description
1059899	When setting <code>sec-default-action</code> to <code>accept</code> 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. <b>Workaround:</b> set <code>sec-default-action</code> to <code>deny</code> first in the CLI and then change the setting to <code>accept</code> .

### Firewall

Bug ID	Description
992610	The source interface displays the name of the VDOM and local out traffic displays as forward traffic.

### FortiGate 6000 and 7000 platforms

Bug ID	Description
1060619	CSF is not working as expected.

## GUI

Bug ID	Description
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 <code>Node.JS</code> daemon restarts with a <code>kill ESRCH</code> error on FortiGate after an upgrade.

## HA

Bug ID	Description
1056138	On the FortiGate 120G and 121G, HA did not synchronize and the GUI HA page stuck loading when <i>ha</i> or <i>mgmt</i> interfaces used as the heartbeat interface. <b>Workaround:</b> do not use <i>ha</i> or <i>mgmt</i> interfaces as the heartbeat interface.
1062433	SASE FortiGate's go out of synchronization after <code>HTTP.Chunk.Length.Invalid</code> was removed in the new FMWP package. <b>Workaround:</b> run the <code>di ips global rule reload</code> command on the FortiGate's.

## Intrusion Prevention

Bug ID	Description
1069190	After upgrading to FortiOS version 7.2.9, FortiGate may experience a CPU usage issue due to IPS engine version 7.00342 when there are large amount of proxy inspected traffic using the application control and IPS sensor. <b>Workaround:</b> downgrade the IPS engine to version 7.00341.

## Routing

Bug ID	Description
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.

## System

Bug ID	Description
1078541	The FortiFirewall 2600F model may become stuck after a fresh image burn. Upgrading from a previous version stills works. <b>Workaround:</b> power cycle the unit.

## User & Authentication

Bug ID	Description
1075627	<p>On the <i>User &amp; Authentication &gt; RADIUS Servers</i> page, the <i>Test Connectivity</i> and <i>Test User Credentials</i> buttons may incorrectly return a <i>Can't contact RADIUS server</i> error message when testing against a RADIUS server that requires the <code>message-authentication</code> attribute in the access request from the FortiGate.</p> <p>This is a GUI display issue as the actual RADIUS connection does send the <code>message-authentication</code> attribute.</p> <p><b>Workaround:</b> confirm if the connection to RADIUS server using the CLI:  <code>diagnose test authserver radius &lt;server&gt; &lt;method&gt; &lt;user&gt; &lt;password&gt;</code></p>
1080234	<p>For FortiGate (versions 7.2.10 and 7.4.5 and later) and FortiNAC (versions 9.2.8 and 9.4.6 and prior) integration, when testing connectivity/user credentials against FortiNAC that acts as a RADIUS server, the FortiGate GUI and CLI returns an <i>invalid secret for the server</i> error.</p> <p>This error is expected when the FortiGate acts as the direct RADIUS client to the FortiNAC RADIUS server due to a change in how FortiGate handles RADIUS protocol in these versions. However, the end-to-end integration for the clients behind the FortiGate and FortiNAC is not impacted.</p> <p><b>Workaround:</b> confirm the connectivity between the end clients and FortiNAC by checking if the clients can still be authorized against the FortiNAC as normal.</p>

## Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.2.10.

### Anti Virus

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

### Explicit Proxy

Bug ID	Description
865828	The <code>internet-service6-custom</code> and <code>internet-service6-custom-group</code> options do not work with custom IPv6 addresses.
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	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.

Bug ID	Description
	<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> <pre>diagnose wad toggle</pre> <p>(use direct connect diagnose)</p>

## Firewall

Bug ID	Description
985508	<p>When <code>allow-traffic-redirect</code> is enabled, redirect traffic that ingresses and egresses from the same interface may incorrectly get dropped if the source address of the incoming packet is different from the FortiGate's interface subnet and there is no firewall policy to allow the matched traffic.</p> <p><b>Workaround:</b> disable <code>allow-traffic-redirect</code> and create a firewall policy to allow traffic to ingress and egress for the same interface.</p> <pre>config system global     set allow-traffic-redirect disable end</pre>

## 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 <code>uninterruptible-upgrade</code>, 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. For best results, both chassis should be running the same firmware version, although as described above, this is not a requirement.</p>
954881	Image synchronization failure happened after a factory reset on FortiGate 7000E/F .
976521	On FortiGate 6000 models, a CPU usage issue occurs in the node process when navigating a policy list with a large number (+7000) of policies in a VDOM.
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.
1056894	On FortiGate, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.
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 <code>session-sync-dev</code> 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 <code>session-sync-dev</code> command from <code>mgmt-vdom</code> to <code>vsys_ha</code> 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 <code>session-sync-dev</code> to <code>mgmt-vdom</code> 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>

## 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.

Bug ID	Description
854180	On the policy list page, all policy organization with sequence and label grouping is lost.
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).
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.

## HA

Bug ID	Description
988944	On the <i>Fabric Management</i> page, the HA Secondary lists both primary and secondary FortiGate units.
998004	When the HA management interface is set a LAG, it is not synchronized to newly joining secondary HA devices.
1056138	On FortiGate 90G, 91G, 120G, and 121G models in an HA cluster, if the <code>ha</code> or <code>mgmt</code> interface is used as the heartbeat interface, the HA cluster may not synchronize and the GUI HA page may not load. <b>Workaround:</b> do not use <code>ha</code> or <code>mgmt</code> interface as heartbeat interface.
1072440	On FortiGate 90G and 91G models 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. <b>Workaround:</b> configure a valid HA password for the cluster before the upgrade, or manually upgrade the member that was impacted.  <pre>config system ha     set password &lt;new-password&gt; end</pre> <div>  <p>Note that setting the password will cause a HA cluster re-election to occur.</p> </div>

## Hyperscale

Bug ID	Description
802182	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) failed</code> may appear.
817562	NPD/LPMD cannot differentiate the different VRF's, considers as VRF 0 for all.
824071	ECMP does not load balance IPv6 traffic between two routes in a multi-VDOM setup.

Bug ID	Description
843197	Output of <code>diagnose sys npu-session list/list-full</code> does not mention policy route information.
853258	Packets drop, and different behavior occurs between devices in an HA pair with ECMP next hop.
872146	The <code>diagnose sys npu-session list</code> command shows an incorrect policy ID when traffic is using an intra-zone policy.
920228	NAT46 NPU sessions are lost and traffic drops when a HA failover occurs.

## IPsec VPN

Bug ID	Description
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.

## Log & Report

Bug ID	Description
1001583	The GUI is slow and reverts the input when multiple ports are added to a filter for destination ports.

## 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 members can be out-of-sla after some retrieve times.

Bug ID	Description
903444	The <code>diagnose ip rtcache list</code> command is no longer supported in the FortiOS 4.19 kernel.
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.

## Security Fabric

Bug ID	Description
1021684	On the <i>Security Fabric &gt; Physical Topology</i> and <i>Security Fabric &gt; Logical Topology</i> pages, the topology results do not load properly and displays an error.
1057862	FortiGate models with 2GB of memory that manage many extension devices (FortiSwitches and FortiAPs) may enter conserve mode due to the Node process experiencing a memory usage issue over time. <b>Workaround:</b> Avoid loading <i>Security Fabric</i> widget, <i>Security Rating</i> , and <i>Topology</i> pages.

## SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.
941676	Japanese key input does not work correctly during RDP in SSL VPN web mode.

## Switch Controller

Bug ID	Description
947351	The FortiSwitch topology is not loading correctly on the GUI.
961142	An interface in FortiLink is flapping with MCLAG with DAC on an OPSFPP-T-05-PAB transceiver.

## System

Bug ID	Description
782710	Traffic going through a VLAN over VXLAN is not offloaded to NP7.
860460	On a redundant interface, traffic may drop with some NPU-offload enabled policies when the interface is not initialized properly.
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.



Bug ID	Description
901621	<p>On the NP7 platform, setting the interface configuration using <code>set inbandwidth &lt;x&gt;</code> or <code>set outbandwidth &lt;x&gt;</code> commands stops traffic flow.</p> <p><b>Workaround:</b> unset the <code>inbandwidth</code> and <code>outbandwidth</code> in the CLI:</p> <pre>config system interface     edit &lt;port&gt;         unset inbandwidth         unset outbandwidth     next end</pre>
921604	On the FortiGate 601F, the ports (x7) have no cables attached but the link LEDs are green.
1020921	<p>When configuring an SNMP trusted host that matches the management <i>Admin</i> trusted host subnet, the GUI may give an incorrect warning that the current SNMP trusted host does not match. This is purely a GUI display issue and does not impact the actual SNMP traffic.</p> <p><b>Workaround:</b> If the trusted host is enabled on all administrative access, make sure the SNMP host IP is included in at least one of these trusted IP/subnets.</p>

## Upgrade

Bug ID	Description
1055486	<p>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.</p> <p><b>Workaround:</b> initiate the Fabric Upgrade using the CLI.</p>

## User & Authentication

Bug ID	Description
667150	<p>When a remote LDAP user with Two-factor Authentication enabled and Authentication type 'FortiToken' tries to access the internet through firewall authentication, the web page does not receive the FortiToken notification or proceed to authenticate the user.</p> <p><b>Workaround:</b> click the <i>Continue</i> button on the authentication page after approving the FortiToken on the mobile device.</p>
1043189	<p>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.</p> <p>For example, the <i>Users and Devices</i> page or FortiNAC request can trigger the following API call that causes the <code>httpsd</code> process encounter a CPU usage issue and memory usage issue.</p> <pre>GET request /api/v2/monitor/user/device/query</pre>

## 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.

## Web Filter

Bug ID	Description
885222	HTTP session is logged as HTTPS in web filter when VIP is used.

## 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 <code>acd-process-count</code> is not zero).
869978	CAPWAP tunnel traffic over tunnel SSID is dropped when offloading is enabled.
873273	The <i>Automatically connect to nearest saved network</i> option does not work as expected when FWF-60E client-mode local radio loses connection.
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP devices (over 50). This issue does not impact FortiAP management and operation.
941691	Managed FortiSwitch detects multiple MACs using the same IP address.
1001104	Some FortiAP 231F units show join/leave behavior after the FortiGate is upgraded to 7.2.7.
1031659	WiFi clients are disconnected from SSIDs due to an error condition in the daemon hostapd process.
1050915	When upgrading more than 30 managed FortiAPs at the same time using the <i>Managed FortiAP</i> page, the GUI may become slow and unresponsive when selecting the firmware. <b>Workaround:</b> Upgrade the FortiAPs in smaller batches of up to 20 devices to avoid performance impacts.

## ZTNA

Bug ID	Description
819987	SMB drive mapping made through a ZTNA access proxy is inaccessible after rebooting.

## Built-in AV Engine

AV Engine 6.00301 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

## Built-in IPS Engine

IPS Engine 7.00342 is released as the built-in IPS Engine. Refer to the [IPS Engine Release Notes](#) for information.

# 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.



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

Copyright© 2024 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.