

Release Notes

FortiOS 7.2.7



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



March 6, 2024

FortiOS 7.2.7 Release Notes

01-727-986082-20240306

TABLE OF CONTENTS

Change Log	5
Introduction and supported models	6
Supported models	6
Special branch supported models	6
FortiGate 6000 and 7000 support	7
Special notices	8
IPsec phase 1 interface type cannot be changed after it is configured	8
IP pools and VIPs are now considered local addresses	8
FortiGate 6000 and 7000 incompatibilities and limitations	8
Hyperscale incompatibilities and limitations	9
Remove support for SHA-1 certificate used for web management interface (GUI)	9
SMB drive mapping with ZTNA access proxy	9
Console error message when FortiGate 40xF boots	9
FortiGate models with 2 GB RAM cannot be a Security Fabric root	10
FortiGuard Web Filtering Category v10 update	10
FortiAP-W2 models may experience bootup failure during automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port	12
Upgrade information	13
Fortinet Security Fabric upgrade	13
Downgrading to previous firmware versions	14
Firmware image checksums	15
Strong cryptographic cipher requirements for FortiAP	15
FortiGate VM VDOM licenses	15
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name	15
FortiGate 6000 and 7000 upgrade information	16
IPS-based and voipd-based VoIP profiles	17
Upgrade error message	18
BIOS-level signature and file integrity checking during downgrade	19
Product integration and support	20
Virtualization environments	21
Language support	21
SSL VPN support	22
SSL VPN web mode	22
Resolved issues	23
Common Vulnerabilities and Exposures	23
Known issues	24
Anti Virus	24
Explicit Proxy	24
Firewall	24

FortiGate 6000 and 7000 platforms	25
FortiView	27
GUI	27
Hyperscale	27
IPsec VPN	28
Log & Report	28
Proxy	28
Remote Access	29
Routing	29
Security Fabric	29
SSL VPN	29
System	30
Upgrade	30
VM	31
Web Filter	31
WiFi Controller	31
ZTNA	31
Built-in AV Engine	32
Limitations	33
Citrix XenServer limitations	33
Open source XenServer limitations	33

Change Log

Date	Change Description
2024-02-07	Initial release.
2024-02-08	Added Resolved issues on page 23 and Built-in AV Engine on page 32 . Updated Known issues on page 24 and FortiGate models with 2 GB RAM cannot be a Security Fabric root on page 10 .
2024-02-09	Updated FortiGate 6000 and 7000 upgrade information on page 16 .
2024-02-12	Updated Resolved issues on page 23 and Known issues on page 24 .
2024-02-13	Updated Known issues on page 24 .
2024-02-20	Updated Known issues on page 24 .
2024-02-23	Added FortiAP-W2 models may experience bootup failure during automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port on page 12 and BIOS-level signature and file integrity checking during downgrade on page 19 .
2024-02-26	Updated FortiAP-W2 models may experience bootup failure during automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port on page 12 .
2024-03-06	Updated Known issues on page 24 .

Introduction and supported models

This guide provides release information for FortiOS 7.2.7 build 1577.

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

Supported models

FortiOS 7.2.7 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-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-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
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	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
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 7.2.7. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1577.

FFW-1801F	is released on build 6041.
------------------	----------------------------

FFW-2600F	is released on build 6041.
FFW-4200F	is released on build 6041.
FFW-4400F	is released on build 6041.
FFW-4401F	is released on build 6041.
FFW-4801F	is released on build 6041.

FortiGate 6000 and 7000 support

FortiOS 7.2.7 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

- [IPsec phase 1 interface type cannot be changed after it is configured on page 8](#)
- [IP pools and VIPs are now considered local addresses on page 8](#)
- [FortiGate 6000 and 7000 incompatibilities and limitations on page 8](#)
- [Hyperscale incompatibilities and limitations on page 9](#)
- [Remove support for SHA-1 certificate used for web management interface \(GUI\) on page 9](#)
- [SMB drive mapping with ZTNA access proxy on page 9](#)
- [Console error message when FortiGate 40xF boots on page 9](#)
- [FortiGate models with 2 GB RAM cannot be a Security Fabric root on page 10](#)
- [FortiGuard Web Filtering Category v10 update on page 10](#)
- [FortiAP-W2 models may experience bootup failure during automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port 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 7.2.7 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 7.2.7 features.

Remove support for SHA-1 certificate used for web management interface (GUI)

Starting in FortiOS 7.2.5, users should use the built-in Fortinet_GUI_Server certificate or SHA-256 and higher certificates for the web management interface. For example:

```
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

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 7.2.7 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 automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port

Disable automatic firmware upgrades and 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 start 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.

Both automatic firmware upgrade and manually triggering federated upgrade can cause this issue.

For more information about federated upgrade and automatic firmware upgrades, see [Upgrading all device firmware by following the upgrade path \(federated update\)](#) and [Enabling automatic firmware updates](#).

To disable automatic upgrade:

```
config system fortiguard
    set auto-firmware-upgrade disable
end
```

Upgrade information

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

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.2.7 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.2.4
FortiManager	• 7.2.4
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP FortiAP-S FortiAP-U FortiAP-W2	• See Strong cryptographic cipher requirements for FortiAP on page 15
FortiClient* EMS	• 7.0.3 build 0229 or later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 or later
FortiClient* Mac OS X	• 7.0.3 build 0131 or later
FortiClient* Linux	• 7.0.3 build 0137 or later
FortiClient* iOS	• 7.0.2 build 0036 or later
FortiClient* Android	• 7.0.2 build 0031 or later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 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. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor
18. FortiPolicy



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.7. When Security Fabric is enabled in FortiOS 7.2.7, all FortiGate devices must be running FortiOS 7.2.7.

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 7.2.7:



Graceful upgrade of a FortiGate 6000 or 7000 FGCP HA cluster is not supported when upgrading from FortiOS 7.0.12, 7.0.13, or 7.0.14 to 7.2.7.

Upgrading the firmware of a FortiGate 6000 or 7000 FGCP HA cluster from 7.0.12, 7.0.13, or 7.0.14 to 7.2.7 should be done during a maintenance window, since the firmware upgrade process will disrupt traffic for up to 30 minutes.

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.

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 7.2.7 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. Confirm that all components are synchronized and operating normally.
For example, go to *Monitor > Configuration Sync Monitor* to view the status of all components, or use `diagnose sys confsync status` to confirm that all components are synchronized.

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 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 voip profile edit "ips_voip_filter" set feature-set ips next edit "sip_alg_profile" set feature-set voipd next end 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.

Product integration and support

The following table lists FortiOS 7.2.7 product integration and support information:

Web browsers	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	• 5.0 build 0312 and later (needed for FSSO agent support OU in group filters) • Windows Server 2022 Standard • Windows Server 2022 Datacenter • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
AV Engine	• 6.00293
IPS Engine	• 7.00326

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	8.1 Express Edition, Dec 17, 2019
Linux KVM	- Ubuntu 18.0.4 LTS - Red Hat Enterprise Linux release 8.4 - SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	2012R2 with Hyper-V role
Windows Hyper-V Server	2019
Open source XenServer	- Version 3.4.3 - Version 4.1 and later
VMware ESXi	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 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 7.2.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
959918	FortiOS 7.2.7 is no longer vulnerable to the following CVE Reference: • CVE-2023-38545
989429	FortiOS 7.2.7 is no longer vulnerable to the following CVE Reference: • CVE-2024-21762
993323	FortiOS 7.2.7 is no longer vulnerable to the following CVE Reference: • CVE-2024-23113

Known issues

The following issues have been identified in version 7.2.7. To inquire about a particular bug or report a bug, please contact [Customer Service & Support](#).

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.
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. Workaround: restart the WAD process, or update the number of WAD processors. <pre>config system global set wad-worker-count <integer> end</pre>
942612	Web proxy forward server does not convert HTTP version to the original version when sending them back to the client.

Firewall

Bug ID	Description
958311	Firewall address list may show incorrect error for an unresolved FQDN address. This is purely a GUI display issue; the FQDN address can be resolved by the FortiGate and traffic can be matched. Workaround: run the following command to check if an FQDN address is being resolved properly. <pre># diagnose test application dnsproxy 7</pre>

FortiGate 6000 and 7000 platforms

Bug ID	Description
638799	The DHCPv6 client does not work with vcluster2.
781163	<i>FortiView Sources</i> page is unable to display historical data from FortiAnalyzer due to <i>Fail to retrieve FortiView data</i> error.
790464	Existing ARP entries are removed from all slots when an ARP query of a single slot does not respond.
885205	IPv6 ECMP is not supported for the FG-6000F and FG-7000E platforms. IPv6 ECMP is supported for the FG-7000F platform.
887946	UTM traffic is blocked by an FGSP configuration with asymmetric routing.
907695	The FortiGate 6000 and 7000 platforms do not support IPsec VPN over a loopback interface or an NPU inter-VDOM link interface.
910883	The FortiGate 6000s or 7000s in an FGSP cluster may load balance FTP data sessions to different FPCs or FPMs. This can cause delays while the affected FortiGate 6000 or 7000 re-installs the sessions on the correct FPC or FPM.
937879	FortiGate 7000F chassis with FIM-7941Fs cannot load balance fragmented IPv6 TCP and UDP traffic. Instead, fragmented IPv6 TCP and UDP traffic received by the FIM-7941F interfaces is sent directly to the primary FPM, bypassing the NP7 load balancers. IPv6 ICMP fragmented traffic load balancing works as expected. Load balancing fragmented IPv6 TCP and UDP traffic works as expected in FortiGate 7000F chassis with FIM-7921Fs.
941944	CPU usage data displayed on the FortiGate 6000 GUI is actually CPU usage data for the management board. CPU usage data displayed on the FortiGate 7000 GUI is actually the CPU usage for the primary FIM. Use the global <code>get system performance status</code> command to display CPU usage and other performance information for all components (on the FortiGate 6000 the management board and all FPCs, or on the FortiGate 7000 the FIMs and FPMs). This command also displays global performance information including: <pre> Dataplane CPU states: 1% Dataplane memory states: 21% Dataplane average sessions: 8720 sessions in 1 minute Dataplane average session setup rate: 4632 sessions per second in last 1 minute </pre>
946943	On 6K and 7K platforms, the management VDOM GUI should not show the <i>WiFi & Switch Controller</i> menu.
948388	On the FortiGate 6000s, missing image update command in the CLI: <code>execute load-balance update image</code> .
948750	When EMAC VLAN interfaces are removed spontaneously from the configuration, TCP traffic through their underlying VLAN interface fails.

Bug ID	Description
949175	On the FortiGate 7121F, with FIM2 as the primary FIM, making FIM1 the primary causes NP7 PLE invalidation.
949240	SLBC special ports will not match local-in policy in the management path.
951135	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. 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. 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.
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. 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. 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.
954862	Graceful upgrade from 7.0.12 to 7.2.6 or 7.2.7, or from 7.0.12 to 7.4.2 or 7.4.3 will fail on the FortiGate 6501F/6500F, FortiGate 7060E with slot6 occupied, and FortiGate 7121F with slot12 occupied. Workaround: Disable <code>uninterruptible-upgrade</code> before performing the firmware upgrade: <pre>config system ha set uninterruptible-upgrade disable end</pre> Note that traffic will be interrupted for 15 to 45 minutes, depending on the size of the configurations.
954881	Image synchronization failure happened after a factory reset on FortiGate 7000E/F .
973407	FIM installed NPU session causes the SSE to get stuck.
978241	FortiGate does not honor worker port partition when SNATing connections using a fixed port range IP pool.

FortiView

Bug ID	Description
941521	On the <i>FortiView Web Sites</i> page, the <i>Category</i> filter does not work in the Japanese GUI.

GUI

Bug ID	Description
848660	Read-only administrator may encounter a <i>Maximum number of monitored interfaces reached</i> error when viewing an interface bandwidth widget for an interface that does not have the monitor bandwidth feature enabled. Workaround: super_admin users can enable the monitor bandwidth feature on the interface first, then the widget can work for read-only administrators.
853352	On the <i>View/Edit Entries</i> slide-out pane (<i>Policy & Objects > Internet Service Database</i> dialog), users cannot scroll down to the end if there are over 100000 entries.
854180	On the policy list page, all policy organization with sequence and label grouping is lost.
934644	When the FortiGate is in conserve mode, node process (GUI management) may not release memory properly causing entry-level devices to stay in conserve mode.
974988	FortiGate GUI should not show a license expired notification due to an expired device-level FortiManager Cloud license if it still has a valid account-level FortiManager Cloud license (function is not affected).

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.
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.

Bug ID	Description
920228	NAT46 NPU sessions are lost and traffic drops when a HA failover occurs.
949188	With NAT64 HS policy, ICMP reply packets are dropped by FortiOS.
950582	Traffic not passing across the VDOM link.
958066	Observed TCP sessions timing out with a single hyperscale VDOM configuration after loading image from BIOS.

IPsec VPN

Bug ID	Description
852051	IPsec is not fully offloaded, and IPsec VPN throughput is poor.

Log & Report

Bug ID	Description
932537	If Security Rating is enabled to run on schedule (every four hours), the FortiGate can unintentionally send local-out traffic to fortianalyzer.forticloud.com during the Security Rating run. Workaround: disable on-schedule Security Rating run. <pre>config system global set security-rating-run-on-schedule disable end</pre>
960661	FortiAnalyzer report is not available to view for the secondary unit in the HA cluster. Workaround: view the report directly in FortiAnalyzer.
965247	FortiGate syslog format in reliable transport mode is not compliant with RFC 6587.

Proxy

Bug ID	Description
790426	An error case occurs in WAD while redirecting the web filter HTTPS sessions.
828917	Unexpected behavior in WAD when there are multiple LDAP servers configured on the FortiGate.
845361	When a client opens two files and sends a compounded request to read and close file A, this causes file B to be closed twice and WAD to crash.

Bug ID	Description
954104	An error case occurs in WAD when WAD gets the external authenticated users from other daemons.

Remote Access

Bug ID	Description
837391	FortiClient does not send the public IP address for SAML, resulting in <code>0.0.0.0</code> being shown in FortiOS and SASE.

Routing

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

Security Fabric

Bug ID	Description
902344	When there are over 30 downstream FortiGates in the Security Fabric, the root FortiGate's GUI may experience slowness when loading the <i>Fabric Management</i> page and prevents the user from upgrading firmware in the GUI. Workaround: perform the firmware upgrade in the CLI. To perform the firmware upgrade via the GUI, temporarily disable the Security Fabric on the root FortiGate.

SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.
879329	Destination address of SSL VPN firewall policy may be lost after upgrading when <code>dstaddr</code> is set to <code>all</code> and at least one authentication rule has a portal with split tunneling enabled.
947210	Application <code>sslvpn</code> *** <code>code requested backtrace</code> *** was observed during graceful upgrade.

System

Bug ID	Description
861962	When configuring an 802.3ad aggregate interface with a 1 Gbps speed, the port's LED is off and traffic cannot pass through. Affected platforms: 110xE, 220xE, 330xE, 340xE, and 360xE.
882187	Optimize memory usage caused by the high volume of disk traffic logs.
887940	Status light is not showing on the FortiGate 60F or 100F after a cold and warm reboot.
901621	Setting the interface configuration <code>inbandwidth</code> or <code>outbandwidth</code> commands stops traffic flow.
931299	When the URL filter requests the FortiGuard (FGD) rating server address using DNS, it will try to get both A (IPv4) and AAAA (IPv6) records.
937982	High CPU usage might be observed on entry-level FortiGates if the cache size reaches 10% of the system memory.
939013	SNMP walk of the entire MIB fails when the configuration has split-port and a large number of interfaces.
947240	FortiGate is not able to resolve ARPs of few hosts due to their ARP replies not reaching the primary FPM.
963600	SolarWinds is unable to negotiate encryption. A <code>Negotiation failed: no matching host key type found</code> error message appears in the log.
967171	The <code>speed 1000auto</code> setting on ports X1 to X4 disappears after upgrading from 7.2.5 to 7.2.6. Affected platforms: FG-40xF and FG-60xF.
967436	DAC cable between FortiGate and FortiSwitch stops working after upgrading from 7.2.6 to 7.2.7.

Upgrade

Bug ID	Description
939011	On the FortiGate 6000F, the ALL TP VDOM cannot synchronize because of <code>switch-controller.auto-config.policy</code> .
977281	After the FortiGate in an HA environment is upgraded using the Fabric upgrade feature, the GUI might incorrectly show the status <i>Downgrade to 7.2.X shortly</i>, even though the upgrade has completed. This is only a display issue; the Fabric upgrade will not recur unless it is manually scheduled. Workaround: Confirm the Fabric upgrade status to make sure that it is not enabled: <pre>config system federated-upgrade set status disabled end</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 (over 50). This issue does not impact FortiAP management and operation.
990868	Wireless client connection fails with 4-way handshake invalid 2/4 message.
1001104	Some FortiAP 231F units show join/leave behavior after the FortiGate is upgraded to 7.2.7.

ZTNA

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

Built-in AV Engine

AV Engine 6.00295 is released as the built-in AV Engine. Refer to the [AV 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

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.