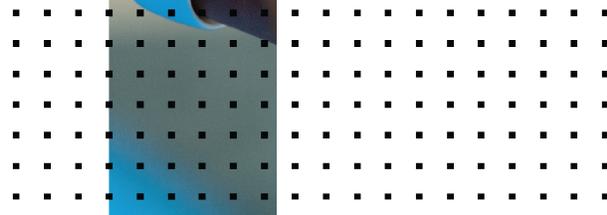


# Release Notes

## FortiOS 7.0.17



**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)



February 17, 2026

FortiOS 7.0.17 Release Notes

01-7017-1108687-20260217

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>5</b>
<b>Introduction and supported models</b> .....	<b>6</b>
Supported models .....	6
Special branch supported models .....	7
<b>Special notices</b> .....	<b>9</b>
Upgrading from older firmware versions .....	9
Azure-On-Demand image .....	9
GCP-On-Demand image .....	9
ALI-On-Demand image .....	10
Unsupported websites in SSL VPN web mode .....	10
RDP and VNC clipboard toolbox in SSL VPN web mode .....	10
CAPWAP offloading compatibility of FortiGate NP7 platforms .....	10
IP pools and VIPs are now considered local addresses .....	11
FEC feature design change .....	11
Hyperscale incompatibilities and limitations .....	11
SMB drive mapping with ZTNA access proxy .....	12
Remote access with write rights through FortiGate Cloud .....	12
Hyperscale NP7 hardware limitation .....	12
HA unsupported between different FortiGate 90G and 91G series hardware generations .....	13
SSL VPN not supported on FortiGate 90G series models .....	14
<b>Upgrade information</b> .....	<b>15</b>
Fortinet Security Fabric upgrade .....	15
Downgrading to previous firmware versions .....	17
Firmware image checksums .....	17
IPsec interface MTU value .....	17
HA role wording changes .....	17
Strong cryptographic cipher requirements for FortiAP .....	18
How VoIP profile settings determine the firewall policy inspection mode .....	18
L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later .....	19
Add interface for NAT46 and NAT64 to simplify policy and routing configurations ..	20
Upgrading .....	20
Creating new policies .....	21
Example configurations .....	21
ZTNA configurations and firewall policies .....	23
Default DNS server update .....	23
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name .....	24
BIOS-level signature and file integrity checking during downgrade .....	24
Upgrading from 7.0.11 or earlier versions .....	25

<b>Product integration and support</b> .....	<b>26</b>
Virtualization environments .....	27
Language support .....	27
SSL VPN support .....	28
SSL VPN web mode .....	28
<b>Resolved issues</b> .....	<b>29</b>
GUI .....	29
REST API .....	29
Routing .....	29
SSL VPN .....	29
Common Vulnerabilities and Exposures .....	30
<b>Known issues</b> .....	<b>31</b>
New known issues .....	31
SSL VPN .....	31
System .....	31
Existing known issues .....	31
Firewall .....	32
FortiView .....	32
GUI .....	33
HA .....	34
Hyperscale .....	34
IPsec VPN .....	35
Log & Report .....	35
Proxy .....	35
Security Fabric .....	35
System .....	36
Upgrade .....	36
VM .....	36
Web Filter .....	37
WiFi Controller .....	37
ZTNA .....	37
<b>Built-in AV Engine</b> .....	<b>38</b>
<b>Built-in IPS Engine</b> .....	<b>39</b>
<b>Limitations</b> .....	<b>40</b>
Citrix XenServer limitations .....	40
Open source XenServer limitations .....	40
Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models .....	40

# Change Log

Date	Change Description
2025-01-14	Initial release.
2025-01-20	Updated <a href="#">Known issues on page 31</a> .
2025-01-21	Updated <a href="#">Special branch supported models on page 7</a> .
2025-01-27	Updated <a href="#">Known issues on page 31</a> .
2025-01-28	Updated <a href="#">Special branch supported models on page 7</a> .
2025-02-03	Updated <a href="#">Known issues on page 31</a> .
2025-03-03	Updated <a href="#">Special branch supported models on page 7</a> .
2025-03-20	Updated <a href="#">Known issues on page 31</a> .
2025-06-12	Updated <a href="#">Resolved issues on page 29</a> .
2025-06-30	Updated <a href="#">Special branch supported models on page 7</a> .
2025-07-10	Updated <a href="#">Resolved issues on page 29</a> .
2025-07-15	Updated <a href="#">Known issues on page 31</a> .
2025-08-01	Updated <a href="#">Known issues on page 31</a> .
2025-08-21	Updated <a href="#">Known issues on page 31</a> .
2025-08-26	Updated <a href="#">Known issues on page 31</a> .
2025-09-23	Updated <a href="#">HA unsupported between different FortiGate 90G and 91G series hardware generations on page 13</a> .
2025-10-15	Updated <a href="#">Resolved issues on page 29</a> .
2026-02-03	Updated <a href="#">Special notices on page 9</a> .
2026-02-17	Updated <a href="#">Resolved issues on page 29</a> .

# Introduction and supported models

This guide provides release information for FortiOS 7.0.17 build 0682.

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

## Supported models

FortiOS 7.0.17 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-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-400F, FG-401F, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, 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-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
<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-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
<b>FortiGate Rugged</b>	FGR-60F, FGR-60F-3G4G
<b>FortiFirewall</b>	FFW-3980E, FFW-VM64, FFW-VM64-KVM
<b>FortiGate VM</b>	FG-ARM64-AWS, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
<b>Pay-as-you-go images</b>	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

## Special branch supported models

The following models are released on a special branch of FortiOS 7.0.17. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0682.

<b>FG-50G</b>	is released on build 7592.
<b>FG-51G</b>	is released on build 7598.
<b>FG-50G-5G</b>	is released on build 7592.
<b>FG-51G-5G</b>	is released on build 7598.
<b>FG-50G-DSL</b>	is released on build 7592.
<b>FG-50G-SFP</b>	is released on build 7592.
<b>FG-50G-SFP-POE</b>	is released on build 7592.
<b>FG-51G-SFP-POE</b>	is released on build 7592.
<b>FG-80F-DSL</b>	is released on build 7569.
<b>FG-90G</b>	is released on build 7571.
<b>FG-91G</b>	is released on build 7571.
<b>FG-120G</b>	is released on build 7572.
<b>FG-121G</b>	is released on build 7572.
<b>FG-900G</b>	is released on build 7573.
<b>FG-901G</b>	is released on build 7573.
<b>FG-1000F</b>	is released on build 7574.
<b>FG-1001F</b>	is released on build 7574.
<b>FG-3200F</b>	is released on build 7575.
<b>FG-3201F</b>	is released on build 7575.
<b>FG-3700F</b>	is released on build 7575.
<b>FG-3701F</b>	is released on build 7575.
<b>FG-4800F</b>	is released on build 7575.
<b>FG-4801F</b>	is released on build 7575.
<b>FGR-50G-5G</b>	is released on build 7577.
<b>FGR-70F</b>	is released on build 7570.
<b>FGR-70F-3G4G</b>	is released on build 7570.
<b>FGR-70G</b>	is released on build 7594.
<b>FGR-70G-5G-DUAL</b>	is released on build 7577.

<b>FWF-80F-2R-3G4G-DSL</b>	is released on build 7569.
<b>FWF-81F-2R-3G4G-DSL</b>	is released on build 7569.
<b>FWF-50G</b>	is released on build 7592.
<b>FWF-51G</b>	is released on build 7598.
<b>FWF-50G-5G</b>	is released on build 7592.
<b>FWF-50G-DSL</b>	is released on build 7592.
<b>FWF-50G-SFP</b>	is released on build 7592.

# Special notices

- [Upgrading from older firmware versions on page 9](#)
- [Unsupported websites in SSL VPN web mode on page 10](#)
- [RDP and VNC clipboard toolbox in SSL VPN web mode on page 10](#)
- [FEC feature design change on page 11](#)
- [Hyperscale incompatibilities and limitations on page 11](#)
- [SMB drive mapping with ZTNA access proxy on page 12](#)
- [Hyperscale NP7 hardware limitation on page 12](#)
- [HA unsupported between different FortiGate 90G and 91G series hardware generations on page 13](#)
- [SSL VPN not supported on FortiGate 90G series models on page 14](#)

## Upgrading from older firmware versions

It is best practices to use the [Upgrade Path Tool](#) to find the recommended upgrade path before performing an upgrade. Additionally, please refer to the following Upgrade Notices for a smooth upgrade.

- [Upgrading from 7.0.11 or earlier versions on page 25](#)

## Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

## GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

## ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

## Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1 and later:

- Facebook
- Gmail
- Office 365
- YouTube

## RDP and VNC clipboard toolbox in SSL VPN web mode

Press F8 to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1 and later.

## CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms running FortiOS 7.0.1 and later, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR,

or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

## IP pools and VIPs are now considered local addresses

In FortiOS 7.0.13 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 7.0.1 to 7.0.12, 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](#).

## FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
  edit <id>
    set fec enable
  next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

## Hyperscale incompatibilities and limitations

See [Hyperscale firewall incompatibilities and limitations](#) in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.0.17 features.

## SMB drive mapping with ZTNA access proxy

In FortiOS 7.0.12 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.

## 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`).

# HA unsupported between different FortiGate 90G and 91G series hardware generations

Because of significant differences in interface naming conventions between Generation 1 and Generation 2 FortiGate 90G and 91G series devices, the high availability (HA) feature is not supported between Generation 1 and Generation 2 of the same devices.

For example, for a Generation 1 FortiGate 91G device, the following output is observed:

```
FortiGate-91-Gen1 # get hardware status
Model name: FortiGate-91G
ASIC version: SOC5
CPU: ARMv8
Number of CPUs: 8
RAM: 7547 MB
EMMC: 9982 MB(MLC) /dev/mmcblk0
Hard disk: 114473 MB /dev/nvme0n1
USB Flash: not available
Network Card chipset: FortiASIC NP7LITE Adapter (rev.)
Hardware Board ID: 002
```

For a Generation 2 FortiGate 91G device, the following output is observed:

```
FortiGate-91G-Gen2 # get hardware status
Model name: FortiGate-91G
ASIC version: SOC5
CPU: ARMv8
Number of CPUs: 8
RAM: 7547 MB
EMMC: 9982 MB(MLC) /dev/mmcblk0
Hard disk: 114473 MB /dev/nvme0n1
USB Flash: 58991 MB
Network Card chipset: FortiASIC NP7LITE Adapter (rev.)
Hardware Board ID: 003
```

Observe the Generation differences are reflected in the differences in *Hardware Board ID*.

In this example, for the Generation 1 FortiGate 91G, the WAN interfaces are wan1 and wan2, respectively. However, for the Generation 2 FortiGate 91G, the WAN interfaces are x1 and x2, respectively. Therefore, because of the differences in interface names, HA cannot be formed between these Generation 1 and Generation 2 devices.



Generation 1 configurations for FortiGate 90G and 91G series devices cannot be applied to Generation 2 FortiGate 90G and 91G series devices.

---

## **SSL VPN not supported on FortiGate 90G series models**

The SSL VPN web and tunnel mode feature will not be available from the GUI or the CLI on the FortiGate 90G and 91G models. Settings will not be upgraded from previous versions.

Consider migrating to using IPsec Dialup VPN for remote access.

# 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 7.0.17 greatly increases the interoperability between other Fortinet products. This includes:

<b>FortiAnalyzer</b>	• 7.0.13
<b>FortiManager</b>	• 7.0.13
<b>FortiExtender</b>	• 7.0.3 and later. For compatibility with latest features, use latest 7.4 version.
<b>FortiSwitch OS (FortiLink support)</b>	• 6.4.6 build 0470 or later
<b>FortiAP FortiAP-S FortiAP-U FortiAP-W2</b>	• See <a href="#">Strong cryptographic cipher requirements for FortiAP on page 18</a>
<b>FortiClient* EMS</b>	• 7.0.0 build 0042 or later
<b>FortiClient* Microsoft Windows</b>	• 7.0.0 build 0029 or later
<b>FortiClient* Mac OS X</b>	• 7.0.0 build 0022 or later
<b>FortiClient* Linux</b>	• 7.0.0 build 0018 or later
<b>FortiClient* iOS</b>	• 6.4.6 build 0507 or later

<b>FortiClient* Android</b>	• 6.4.6 build 0539 or later
<b>FortiSandbox</b>	• 2.3.3 and later

\* 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 7.0.0, use FortiClient 7.0.0.

---

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. FortiADC
13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice
17. FortiDeceptor
18. FortiAI/FortiNDR
19. FortiTester
20. FortiMonitor



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.17. When Security Fabric is enabled in FortiOS 7.0.17, all FortiGate devices must be running FortiOS 7.0.17.

---

## 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*.

## IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
  config ospf-interface
    edit "ipsce-vpnx"
      set mtu-ignore enable
    next
  end
end
```

## HA role wording changes

The term `master` has changed to `primary`, and `slave` has changed to `secondary`. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

## 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
```

## How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

In the case when customers are using the following settings in 6.4:

```
config system settings
    set default-voip-alg-mode proxy-based
end
```

```
config firewall policy
    edit 0
        set inspection-mode flow
        unset voip-profile
    next
end
```

In 6.4, by default, SIP traffic is handled by proxy-based SIP ALG even though no VoIP profile is specified in a firewall policy.

After upgrading, the firewall policy will remain in `inspection-mode flow` but handled is by flow-based SIP inspection.

Due to the difference in which the SIP traffic is handled by flow-based SIP versus proxy-based SIP ALG inspection in 7.0.0 and later, if customers want to maintain the same behavior after upgrading, they can manually change the firewall policy's inspection-mode to proxy:

```
config firewall policy
  edit 0
    set inspection-mode proxy
    unset voip-profile
  next
end
```

Or prior to upgrading, they can assign a voip-profile to the firewall policies that are processing SIP traffic to force the conversion to inspection-mode proxy after upgrading.

## L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later

If the setting is not manually updated after upgrading, the VPN connection will be established, but it will not be accessible from the internal network (office network). This setting change is necessary regardless of whether route-based or policy-based IPsec is used.

### To make L2TP over IPsec work after upgrading:

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
  set eip 210.0.0.254
  set sip 210.0.0.1
  set status enable
  set usrgrp "L2tpusergroup"
end
```

Add a static route after upgrading:

```
config router static
  edit 1
    set dst 210.0.0.0 255.255.255.0
    set device "l2t.root"
  next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

# Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

## Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`
- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects > NAT46 Policy*
- *Policy & Objects > NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects > Virtual IPs* related pages

---

During the upgrade process after the FortiGate reboots, the following message is displayed:



The config file may contain errors,  
Please see details by the command `'diagnose debug config-error-log read'`

The following output is displayed after running the diagnose command:

```
# diagnose debug config-error-log read
>>> "config" "firewall" "policy64" @ root:command parse error (error -61)
>>> "config" "firewall" "policy46" @ root:command parse error (error -61)
```

## Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, you will need to manually create new vip46 and vip64 policies.

- Create a vip46 from `config firewall vip` and enable the nat46 option.
- Create a vip64 from `config firewall vip6` and enable the nat64 option.
- Create or modify `ippool1` and `ippool16`, and enable the nat64 or nat46 option.
- Create a policy and enable the nat46 option, apply the vip46 and `ippool16` in a policy.
- Create a policy and enable the nat64 option, apply the vip64 and `ippool1` in policy.
- Ensure the routing on the client and server matches the new vip/vip6 and `ippool/ippool16`.

## Example configurations

vip46 object:

Old configuration	New configuration
<pre>config firewall vip46   edit "test-vip46-1"     set extip 10.1.100.155     set mappedip 2000:172:16:200::55   next end</pre>	<pre>config firewall vip   edit "test-vip46-1"     set extip 10.1.100.150     set nat44 disable     <b>set nat46 enable</b>     set extintf "port24"     <b>set ipv6-mappedip 2000:172:16:200::55</b>   next end</pre>

ippool6 object:

Old configuration	New configuration
<pre>config firewall ippool6   edit "test-ippool6-1"     set startip 2000:172:16:201::155     set endip 2000:172:16:201::155   next end</pre>	<pre>config firewall ippool6   edit "test-ippool6-1"     set startip 2000:172:16:201::155     set endip 2000:172:16:201::155     <b>set nat46 enable</b>   next end</pre>

NAT46 policy:

Old configuration	New configuration
<pre>config firewall policy46</pre>	<pre>config firewall policy</pre>

Old configuration	New configuration
<pre> edit 1   set srcintf "port24"   set dstintf "port17"   set srcaddr "all"   set dstaddr "test-vip46-1"   set action accept   set schedule "always"   set service "ALL"   set logtraffic enable   set ippool enable   set poolname "test-ippool6-1" next end </pre>	<pre> edit 2   set srcintf "port24"   set dstintf "port17"   set action accept   <b>set nat46 enable</b>   set srcaddr "all"   set dstaddr "test-vip46-1"   set srcaddr6 "all"   set dstaddr6 "all"   set schedule "always"   set service "ALL"   set logtraffic all   set ippool enable   set poolname6 "test-ippool6-1" next end </pre>

vip64 object

Old configuration	New configuration
<pre> config firewall vip64   edit "test-vip64-1"     set extip 2000:10:1:100::155     set mappedip 172.16.200.155   next end </pre>	<pre> config firewall vip6   edit "test-vip64-1"     set extip 2000:10:1:100::155     set nat66 disable     <b>set nat64 enable</b>     <b>set ipv4-mappedip 172.16.200.155</b>   next end </pre>

ippool object

Old configuration	New configuration
<pre> config firewall ippool   edit "test-ippool4-1"     set startip 172.16.201.155     set endip 172.16.201.155   next end </pre>	<pre> config firewall ippool   edit "test-ippool4-1"     set startip 172.16.201.155     set endip 172.16.201.155     <b>set nat64 enable</b>   next end </pre>

NAT64 policy:

Old configuration	New configuration
<pre> config firewall policy64   edit 1     set srcintf "wan2"     set dstintf "wan1"     set srcaddr "all"     set dstaddr "test-vip64-1"     set action accept     set schedule "always"     set service "ALL"     set ippool enable     set poolname "test-ippool4-1"   next end </pre>	<pre> config firewall policy   edit 1     set srcintf "port24"     set dstintf "port17"     set action accept     set nat64 enable     set srcaddr "all"     set dstaddr "all"     set srcaddr6 "all"     set dstaddr6 "test-vip64-1"     set schedule "always"     set service "ALL"     set logtraffic all     set ippool enable     set poolname "test-ippool4-1"   next end </pre>

## ZTNA configurations and firewall policies

Since FortiOS 7.0.2, ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration.

When upgrading from FortiOS 7.0.1 or below:

- If an access-proxy type proxy-policy does not have a srcintf, then after upgrading it will be set to any.
- To display the srcintf as any in the GUI, *System > Feature Visibility* should have *Multiple Interface Policies* enabled.
- All full ZTNA firewall policies will be automatically removed.

## Default DNS server update

Starting in FortiOS 7.0.4, if both primary and secondary DNS servers are set to use the default FortiGuard servers prior to upgrading, the FortiGate will update them to the new servers and enable DoT after upgrading. If one or both DNS servers are not using the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

## 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.

## 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.

## Upgrading from 7.0.11 or earlier versions

Upgrading directly from 7.0.11 or earlier versions to 7.0.15 is not supported.

To upgrade:

1. Check the recommended upgrade path using the [Upgrade Path Tool](#).
2. If upgrading from the GUI, upgrade to each firmware version in the upgrade path using the direct upgrade option.

In the event the system hangs due to following an unsupported upgrade path to version 7.0.15, boot up the backup partition from the BIOS, and follow the instructions above to upgrade again.

# Product integration and support

The following table lists FortiOS 7.0.17 product integration and support information:

<b>FortiManager and FortiAnalyzer</b>	See the <a href="#">FortiOS Compatibility Tool</a> for information about FortiOS compatibility with FortiManager and FortiAnalyzer.
<b>Web browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Edge 114</li><li>• Mozilla Firefox version 113</li><li>• Google Chrome version 114</li></ul> Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
<b>Explicit web proxy browser</b>	<ul style="list-style-type: none"><li>• Microsoft Edge 114</li><li>• Mozilla Firefox version 113</li><li>• Google Chrome version 114</li></ul> Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
<b>FortiController</b>	<ul style="list-style-type: none"><li>• 5.2.5 and later</li></ul> Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
<b>Fortinet Single Sign-On (FSSO)</b>	<ul style="list-style-type: none"><li>• 5.0 build 0319 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none"><li>• Windows Server 2022 Standard</li><li>• Windows Server 2022 Datacenter</li><li>• Windows Server 2019 Standard</li><li>• Windows Server 2019 Datacenter</li><li>• Windows Server 2019 Core</li><li>• Windows Server 2016 Datacenter</li><li>• Windows Server 2016 Standard</li><li>• Windows Server 2016 Core</li><li>• Windows Server 2012 Standard</li><li>• Windows Server 2012 R2 Standard</li><li>• Windows Server 2012 Core</li><li>• Windows Server 2008 64-bit (requires Microsoft SHA2 support package)</li><li>• Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)</li><li>• Windows Server 2008 Core (requires Microsoft SHA2 support package)</li></ul></li><li>• Novell eDirectory 8.8</li></ul>

<b>AV Engine</b>	• 6.00302
<b>IPS Engine</b>	• 7.00187

## 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 ESX</b>	<ul style="list-style-type: none"> <li>Versions 4.0 and 4.1</li> </ul>
<b>VMware ESXi</b>	<ul style="list-style-type: none"> <li>Versions 6.5, 6.7, and 7.0.</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)	✓

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

## GUI

Bug ID	Description
1110382	Admin can login to GUI (HTTPS) with password, even when admin-https-pki-required is enabled.

## REST API

Bug ID	Description
989677	Update JavaScripts to the latest Long Term Support version.

## Routing

Bug ID	Description
935297	Probe server <code>aws.amazon.com</code> is listed in SD-WAN default health-check list.

## SSL VPN

Bug ID	Description
1101837	Insufficient Session Expiration in SSLVPN using SAML authentication.

## Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1093598	FortiOS7.0.17 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-50571</li></ul>
1100972	FortiOS7.0.17 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-52965</li></ul>
1103505	FortiOS 7.0.17 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-55591</li></ul>
1108301	FortiOS 7.0.17 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-22254</li></ul>
1109252	FortiOS7.0.17 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-25252</li></ul>
1112305	FortiOS7.0.17 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-22258</li></ul>

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 31](#)
- [Existing known issues on page 31](#)

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

## New known issues

There are currently no new issues that have been identified in version 7.0.17.

## SSL VPN

Bug ID	Description
1117475	FortiClient cannot dial SSI VPN to FortiGate with SAML login when using an internal browser as the user agent for SAML user authentication.

## System

Bug ID	Description
1117005	CPU spikes and management access issues occur on certain FortiGate models post-upgrade when IPsec Phase 1 NPU-offload is enabled during maintenance.

## Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS7.0.17.

## Firewall

Bug ID	Description
843554	<p>If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of <i>IP</i>, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type <i>IP</i> is created in the GUI.</p> <p>This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service <i>ALL</i> (protocol type <i>IP</i>) as the first service, and this can cause the <i>ALL</i> service to be modified unexpectedly.</p> <p><b>Workaround:</b> create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if <i>ALL</i> is the first firewall service in the list:</p> <pre>config firewall service custom   edit "unused"     set tcp-portrange 1   next   move "unused" before "ALL" end</pre>
912740	<p>On a FortiGate managed by FortiManager, after upgrading to 7.0.13, the <i>Firewall Policy</i> list may show separate sequence grouping for each policy because the <code>global-label</code> is updated to be unique for each policy.</p> <p><b>Workaround:</b> drag and drop the policy to the correct sequence group in the GUI, or remove the <code>global-label</code> for each member policy in the group except for the leading policy.</p> <ul style="list-style-type: none"> <li>• Policy 1 (<code>global-label "group1"</code>)</li> <li>• Policy 2</li> <li>• Policy 3 (<code>global-label "group2"</code>)</li> <li>• Policy 4</li> </ul>
951984	For local out DNAT traffic, the best output route may not be found.

## FortiView

Bug ID	Description
941521	On the <i>Dashboard &gt; FortiView Websites</i> page, the <i>Category</i> filter does not work in the Japanese GUI.

## GUI

Bug ID	Description
440197	On the <i>System &gt; FortiGuard</i> page, the override FortiGuard server for <i>AntiVirus &amp; IPS Updates</i> shows an <i>Unknown</i> status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the <i>Network &gt; Interfaces</i> page when VDOM mode is enabled, the <i>Global</i> view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as UP. The VDOM view shows the correct status.
685431	On the <i>Policy &amp; Objects &gt; Firewall Policy</i> page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. <b>Workaround:</b> use the CLI to configure policies.
707589	<i>System &gt; Certificates</i> list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. <b>Workaround:</b> use Chrome, Edge, or Safari as the browser.
755177	When upgrading firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
810225	An <i>undefined</i> error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
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.
881678	On the <i>Network &gt; Routing Objects</i> page, editing a prefix list with a large number of rule entries fails with an error notification that <i>The integer value is not within valid range</i> . <b>Workaround:</b> edit a prefix list with a large number of rule entries in the CLI.
898902	In the <i>System &gt; Administrators</i> dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the <i>Two-factor Authentication</i> toggle. This issue does not affect configuring other settings in the dialog. <b>Workaround:</b> use the CLI to configure two-factor-authentication under <code>config system admin</code> .
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).

## HA

Bug ID	Description
1102588	<p>On FortiGate 12xG and 9xG series devices, graceful upgrade for the secondary node in a cluster fails when the security level is set to high.</p> <p><b>Workaround:</b> disable HA cluster and upgrade separately, or lower the security level, do the upgrade, and then change the security level back to high.</p>

## Hyperscale

Bug ID	Description
771857	Firewall virtual IP (VIP) features srcfltr, srcintf-fltr, service, arp-reply, nat-source-vip, and portforwarding are not supported by hyperscale firewall policies even though they are visible from the CLI or GUI when configuring IPv4 and IPV6 firewall VIPs in a hyperscale firewall VDOM.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.
836976	Sessions being processed by hyperscale firewall policies with hardware logging may be dropped when dynamically changing the log-processor setting from hardware to host for the hardware log sever added to the hyperscale firewall policy. To avoid dropping sessions, change the log-processor setting during quiet periods.
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
842659	srcaddr-negate and dstaddr-negate are not working properly for IPv6 traffic with FTS.
843132	Access control list (ACL) policies added to a hyperscale firewall VDOM that is processing traffic may take longer than expected to become effective. During a transition period, traffic that should be blocked by the new ACL policy will be allowed.
843197	The npu-session list fails to display policy-route information when traffic is routed through a policy route on FortiGate models using NPU acceleration.
843266	Diagnose command should be available to show hit_count/last_used for policy route and NPU session on hyperscale VDOM.
843305	Get PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS console error log when system boots up.
844421	The diagnose firewall ippool list command does not show the correct output for overload type IP pools.
845269	When editing a Hyperscale firewall policy with an overload CGN IP Pool, the GUI disables endpoint independent filtering cgn-eif regardless if it is enabled or not.
846520	NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover.

Bug ID	Description
895951	The output of the <code>diagnose sys npu-session stat</code> command incorrectly shows a setup rate of 0 for EIF sessions.
941784	Hardware session synchronization does not work on FG-480xF devices in hyperscale.
986656	On the HA primary unit, the <code>npu-session list</code> shows many sessions, but the <code>npu-session state</code> shows 0.
993343	In a Hyperscale VDOM, an interruption in the kernel occurs with <code>set nat46-generate-ipv6-fragment-header</code> enabled.
1024902	After FTP traffic passes, the <code>npu-session stat</code> does not display the accurate amount of actual sessions on FortiGate.

## IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
945367	Disabling <code>src-check (RPF)</code> on the parent tunnel is not inherited by ADVPN shortcuts.

## Log & Report

Bug ID	Description
850642	Logs are not seen for traffic passing through the firewall caused by numerous simultaneous configuration changes.

## Proxy

Bug ID	Description
1001497	FortiGate may enter conserve mode when posting a non or invalid HTTP date through web proxy.

## Security Fabric

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

Bug ID	Description
794703	Security Rating report for <i>Rogue AP Detection</i> and <i>FortiCare Support</i> checks show incorrect results.
862424	On a FortiGate that has large tables (over 1000 firewall policies, address, or other tables), security rating reports may cause the FortiGate to go into conserve mode.
903922	Security Fabric physical and logical topology is slow to load when there are a lot of downstream devices, including FortiGates, FortiSwitches, FortiAPs, and endpoint device traffic. This is a GUI only display issue and does not impact operations of downstream devices.

## System

Bug ID	Description
847664	Console may display <code>mce: [Hardware Error]</code> error message after fresh image burn or reboot.
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.
934708	The <code>cmdbsvr</code> could not secure the <code>var_zone</code> lock due to another process holding it indefinitely.
935158	The FortiGate console prints <code>check_gui_redir_file: No such file or directory</code> after rebooting.
975496	FortiGate 200F experiences slow download and upload speeds when traversing from a 1G to a 10G interface.

## Upgrade

Bug ID	Description
1082256	Received <i>System file integrity check failed!</i> message when upgrading from 7.0.15 to 7.0.16 with BIOS security level 2.

## VM

Bug ID	Description
800935	ESXi VLAN interface based on LACP does not work.

Bug ID	Description
1082304	FortiGate VMs for ARM64 KVM, AWS, OCI, and for VM64 OPC, encounter an error condition in the kernel when performing an upgrade from version 7.0.15 to 7.0.16. The OCI baremetal kernel image is not supported in version 7.0.16 during an upgrade from versions 7.0.13, 7.0.14, or 7.0.15.

## Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

## WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the <i>Managed FortiAPs</i> page and <i>FortiAP Status</i> widget can take a long time to load. This issue does not impact FortiAP operation.
1004338	After an upgrade or reboot on the NP7 platform, WiFi data cannot pass through when the SSID VLAN interface uses the DHCP Relay Server.

## ZTNA

Bug ID	Description
819987	Mapped drives become inaccessible after laptop reboots when using FortiGate ZTNA access proxy with FQDN destinations.
848222	ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type. An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found.

# Built-in AV Engine

AV Engine 6.00302 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

# Built-in IPS Engine

IPS Engine 7.00187 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.

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

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

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

The following HA clusters can be formed:

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

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



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

Copyright© 2026 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.