



# Release Notes

FortiOS 7.6.7



**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](mailto:techdoc@fortinet.com)



June 15, 2026

FortiOS 7.6.7 Release Notes

01-767-1284778-20260615

# TABLE OF CONTENTS

|                                                                                          |           |
|------------------------------------------------------------------------------------------|-----------|
| <b>Change Log</b>                                                                        | <b>6</b>  |
| <b>Introduction and supported models</b>                                                 | <b>7</b>  |
| Supported models                                                                         | 7         |
| FortiGate 6000 and 7000 support                                                          | 7         |
| <b>Special notices</b>                                                                   | <b>9</b>  |
| FortiGate cannot restore configuration file after private-data-encryption is re-enabled  | 9         |
| FortiManager support for updated FortiOS private data encryption key                     | 10        |
| Hyperscale incompatibilities and limitations                                             | 11        |
| Hyperscale NP7 hardware limitation                                                       | 11        |
| FortiGate 6000 and 7000 incompatibilities and limitations                                | 12        |
| FortiGate VM memory and upgrade                                                          | 12        |
| RADIUS vulnerability                                                                     | 12        |
| Changes to NP7 traffic shaping                                                           | 13        |
| SSL VPN tunnel mode replaced with IPsec VPN                                              | 13        |
| Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models  | 14        |
| 2 GB RAM FortiGate models no longer support most FortiOS proxy-related features          | 14        |
| 2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology | 15        |
| GUI access conflict with IPSec TCP tunnel on the same interface                          | 15        |
| SAML certificate verification                                                            | 16        |
| Policy check required for hairpin traffic                                                | 16        |
| Changing vlan-lookup-cache requires system restart                                       | 17        |
| <b>Changes in CLI</b>                                                                    | <b>18</b> |
| <b>Changes in default behavior</b>                                                       | <b>19</b> |
| <b>Changes in default values</b>                                                         | <b>21</b> |
| <b>Changes in table size</b>                                                             | <b>22</b> |
| <b>New features or enhancements</b>                                                      | <b>23</b> |
| FortiASIC                                                                                | 23        |
| GUI                                                                                      | 24        |
| Hyperscale                                                                               | 24        |
| LAN Edge                                                                                 | 25        |
| Network                                                                                  | 25        |
| Policy & Objects                                                                         | 26        |
| Security Fabric                                                                          | 26        |
| Security Profiles                                                                        | 27        |
| System                                                                                   | 27        |
| VPN                                                                                      | 28        |
| ZTNA                                                                                     | 29        |
| <b>Upgrade information</b>                                                               | <b>30</b> |
| Fortinet Security Fabric upgrade                                                         | 30        |

|                                                                                    |           |
|------------------------------------------------------------------------------------|-----------|
| Downgrading to previous firmware versions .....                                    | 32        |
| Firmware image checksums .....                                                     | 32        |
| FortiGate 6000 and 7000 upgrade information .....                                  | 32        |
| Default setting of cp-accel-mode is changed to none on 2GB memory models .....     | 33        |
| Policies that use an interface show missing or empty values after an upgrade ..... | 34        |
| Managed FortiSwitch do not permit empty passwords for administrator accounts ..... | 34        |
| Removed speed setting affects SFP+ interfaces after upgrade .....                  | 35        |
| Hyperscale with FGCP HA clusters and interface monitoring .....                    | 35        |
| Password policy enforcement .....                                                  | 35        |
| <b>Product integration and support .....</b>                                       | <b>37</b> |
| Virtualization environments .....                                                  | 38        |
| Language support .....                                                             | 38        |
| Agentless VPN support .....                                                        | 39        |
| FortiExtender modem firmware compatibility .....                                   | 39        |
| <b>Resolved issues .....</b>                                                       | <b>42</b> |
| Agentless VPN .....                                                                | 42        |
| AntiVirus .....                                                                    | 42        |
| Application Control .....                                                          | 43        |
| DNS Filter .....                                                                   | 43        |
| Endpoint Control .....                                                             | 43        |
| Explicit Proxy .....                                                               | 44        |
| File Filter .....                                                                  | 44        |
| Firewall .....                                                                     | 44        |
| FortiGate 6000/7000 Platform .....                                                 | 46        |
| GUI .....                                                                          | 46        |
| HA .....                                                                           | 49        |
| HyperScale .....                                                                   | 50        |
| IPsec VPN .....                                                                    | 51        |
| Intrusion Prevention .....                                                         | 52        |
| Log and Report .....                                                               | 53        |
| Proxy .....                                                                        | 54        |
| Routing .....                                                                      | 54        |
| SD-WAN .....                                                                       | 55        |
| Security Fabric .....                                                              | 56        |
| Switch Controller .....                                                            | 56        |
| System .....                                                                       | 57        |
| Upgrade .....                                                                      | 61        |
| User and Authentication .....                                                      | 62        |
| VM .....                                                                           | 63        |
| VoIP .....                                                                         | 64        |
| Wan Optimization .....                                                             | 64        |
| Web Filter .....                                                                   | 64        |
| WiFi Controller .....                                                              | 65        |
| ZTNA .....                                                                         | 66        |

---

|                                   |           |
|-----------------------------------|-----------|
| <b>Known issues</b>               | <b>67</b> |
| New known issues                  | 67        |
| HyperScale                        | 67        |
| System                            | 67        |
| Existing known issues             | 67        |
| Agentless VPN                     | 68        |
| Endpoint Control                  | 68        |
| Firewall                          | 68        |
| FortiGate 6000/7000 Platform      | 68        |
| FortiView                         | 69        |
| GUI                               | 69        |
| HA                                | 69        |
| HyperScale                        | 70        |
| IPsec VPN                         | 70        |
| Intrusion Prevention              | 70        |
| Proxy                             | 70        |
| REST API                          | 71        |
| Security Fabric                   | 71        |
| Switch Controller                 | 71        |
| System                            | 71        |
| User and Authentication           | 72        |
| VM                                | 72        |
| Web Filter                        | 72        |
| <b>Built-in AV Engine</b>         | <b>73</b> |
| <b>Built-in IPS Engine</b>        | <b>74</b> |
| <b>Limitations</b>                | <b>75</b> |
| Citrix XenServer limitations      | 75        |
| Open source XenServer limitations | 75        |

# Change Log

| Date       | Change Description                                                                                                                                                                                                                                                                                                      |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2026-06-02 | Initial release.                                                                                                                                                                                                                                                                                                        |
| 2026-06-02 | Updated <a href="#">Introduction and supported models on page 7</a> , <a href="#">Changes in CLI on page 18</a> , <a href="#">New features or enhancements on page 23</a> , <a href="#">Resolved issues on page 42</a> , <a href="#">Known issues on page 67</a> , and <a href="#">Built-in IPS Engine on page 74</a> . |
| 2026-06-03 | Updated <a href="#">Introduction and supported models on page 7</a> .                                                                                                                                                                                                                                                   |
| 2026-06-04 | Updated <a href="#">Resolved issues on page 42</a> , <a href="#">Known issues on page 67</a> , and <a href="#">Built-in IPS Engine on page 74</a> .                                                                                                                                                                     |
| 2026-06-08 | Updated <a href="#">Changes in default behavior on page 19</a> , <a href="#">New features or enhancements on page 23</a> , <a href="#">Resolved issues on page 42</a> , and <a href="#">Known issues on page 67</a> .                                                                                                   |
| 2026-06-15 | Updated <a href="#">Known issues on page 67</a> .                                                                                                                                                                                                                                                                       |

# Introduction and supported models

This guide provides release information for FortiOS 7.6.7 build 3704.

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

## Supported models

FortiOS 7.6.7 supports the following models.

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FortiGate</b>        | FG-30G, FG-31G, FG-40F, FG-40F-3G4G, FG-50G, FG-50G-5G, FG-50G-SFP, FG-50G-DSL, FG-50G-SFP-POE, FG-51G, FG-51G-5G, FG-51G-SFP-POE, FG-60F, FG-61F, FG-70F, FG-70G, FG-70G-POE, FG-71F, FG-71G, FG-71G-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-200G, FG-201E, FG-201F, FG-201G, 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-700G, FG-701G, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, 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-3800G, FG-3801G, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F |
| <b>FortiWiFi</b>        | FWF-30G, FWF-31G, FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-5G, FWF-50G-SFP, FWF-50G-DSL, FWF-51G, FWF-60F, FWF-61F, FWF-70G, FWF-70G-POE, FWF-71G, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>FortiGate Rugged</b> | FGR-50G-5G, FGR-60F, FGR-60F-3G4G, FGR-60G, FGR-70F, FGR-70G, FGR-70G-5G, FGR-70G-5G-Dual, FGR-70F-3G4G                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>FortiFirewall</b>    | FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>FortiGate VM</b>     | FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## FortiGate 6000 and 7000 support

FortiOS 7.6.7 supports the following FG-6000F, FG-7000E, and FG-7000F models:

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

# Special notices

- FortiGate cannot restore configuration file after private-data-encryption is re-enabled on page 9
- FortiManager support for updated FortiOS private data encryption key on page 10
- Hyperscale incompatibilities and limitations on page 11
- Hyperscale NP7 hardware limitation on page 11
- FortiGate 6000 and 7000 incompatibilities and limitations on page 12
- FortiGate VM memory and upgrade on page 12
- RADIUS vulnerability on page 12
- Changes to NP7 traffic shaping on page 13
- SSL VPN tunnel mode replaced with IPsec VPN on page 13
- Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models on page 14
- 2 GB RAM FortiGate models no longer support most FortiOS proxy-related features on page 14
- 2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology on page 15
- GUI access conflict with IPSec TCP tunnel on the same interface on page 15
- SAML certificate verification on page 16
- Policy check required for hairpin traffic on page 16
- Changing vlan-lookup-cache requires system restart on page 17

## FortiGate cannot restore configuration file after private-data-encryption is re-enabled

In a new enhancement, enabling private-data-encryption will utilize a randomly generated private key. Therefore, FortiGate cannot restore the configuration file in the following sequence:

1. private-data-encryption enabled with random key, and configuration is backed up.
2. private-data-encryption disabled.
3. private-data-encryption enabled again, with new random key.
4. Restore configuration file in step 1.

When disabling private-data-encryption, a warning in the CLI will be displayed:

```
This operation will restore system default data encryption key!
```

```
Previous config files encrypted with the private key cannot be restored after this operation!
```

```
Do you want to continue? (y/n)y
```

# FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal private-data-encryption key. Instead administrators simply enable the command, and a random private-data-encryption key is generated.

How FortiManager 7.6.3 and later works with FortiOS private data encryption keys has changed. This topic covers the changes. See [FortiManager behavior on page 10](#).

## Previous FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
12345678901234567890123456789abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
12345678901234567890123456789abc
Your private data encryption key is accepted.
```

## New FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
Do you want to continue? (y/n)y
Private data encryption key generation succeeded!
```

## FortiManager behavior

FortiManager 7.6.3 can centrally manage FortiGates with the private-data-encryption setting enabled, with the following limitations:

- FortiManager cannot import objects that include the password type attribute.
- FortiManager cannot be used to create NAT and transparent VDOMs.

This applies to FortiGates with private keys that are manually configured in FortiOS 7.6.0 and earlier and private keys that are randomly generated in FortiOS 7.6.1 and later.

FortiManager does not require you to verify the private key of the FortiGate when adding it to FortiManager.

FortiGates that require the protection of private data encryption and need to be managed by FortiManager should follow these procedures on a fresh install.

1. On the FortiGate, enable private-data-encryption.
2. On the FortiManager, add the FortiGate to the Device Manager. FortiManager will not be required to provide the key for PDE, as it will not be importing any password-related settings.
3. Make all configuration changes directly on the FortiManager.
4. Push and install the changes to the FortiGate.

If you require the use of NAT or Transparent VDOMs, you should perform this additional step before the steps above.

1. Enable multi-vdom mode on the FortiGate.
2. Add the VDOMs that you will use on the FortiGate.
3. Follow the above steps to enable private-data-encryption and manage the FortiGate from the FortiManager.

For more information, see the [FortiManager Administration Guide](#).

### **FortiOS upgrade behavior with FortiManager 7.6.2 and earlier**

If in FortiOS 7.4.5 or 7.6.0 the 32-digit hexadecimal private key is enabled, and then the FortiGate device is upgraded to 7.6.1, the 32-digit hexadecimal private-data-encryption key is preserved. As a result, FortiManager 7.6.2 and earlier is aware of the 32-digit hexadecimal private-data-encryption key and can continue to manage the FortiGate device. However, if the private-data-encryption key is enabled after an upgrade of FortiOS to 7.6.1, FortiManager 7.6.2 and earlier no longer can manage FortiGate devices running FortiOS 7.6.1.

## **Hyperscale incompatibilities and limitations**

See [Hyperscale firewall incompatibilities and limitations](#) in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.6.7 features.

## **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 `cgn-resource-quota` option is ignored.

Because of this limitation, under certain rare conditions (for example, only a single server side IP address and port are being used for a large number of sessions), port allocation may fail even if the block usage of the client is less than its quota. In cases such as this, if the client has traffic towards some other servers or ports, additional port allocation can become successful. You can also work around this problem by increasing the IP Pool block size (`cgn-block-size`).

## FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.6.7 features.

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

## FortiGate VM memory and upgrade

FortiGate virtual machines (VMs) are not constrained by memory size and will continue to support all available features after upgrading to FortiOS 7.6.0. However, it is recommended to set up VMs with at least 4 GB of RAM for optimal performance.

## RADIUS vulnerability

Fortinet has resolved a RADIUS vulnerability described in CVE-2024-3596. As a result, firewall authentication, FortiGate administrative GUI authentication, and WiFi authentication may be affected depending on the functionality of the RADIUS server software used in your environment. RFC 3579 contains information on the affected RADIUS attribute, message-authenticator.

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

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

Message-authenticator checking is made mandatory under UDP/TCP. It is not mandatory when using TLS. Therefore, if FortiGate is using UDP/TCP mode without RADSEC, the RADIUS server should be patched to ensure the message-authenticator attribute is used in its RADIUS messages.

### Affected Product Integration

- FortiAuthenticator version 6.6.1 and older
- Third party RADIUS server that does not support sending the message-authenticator attribute

**Solution**

- Upgrade FortiAuthenticator to version 6.6.2, 6.5.6 or 6.4.10 and follow the upgrade instructions: <https://docs.fortinet.com/document/fortiauthenticator/6.6.2/release-notes/859240/upgrade-instructions>
- Upgrade the RADIUS server and/or enable it to send the correct message-authenticator attribute

## Changes to NP7 traffic shaping

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

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

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

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

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

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

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

## SSL VPN tunnel mode replaced with IPsec VPN

Starting in FortiOS 7.6.3, the SSL VPN tunnel mode feature is replaced with IPsec VPN, which can be configured to use TCP port 443. SSL VPN tunnel mode is no longer available in the GUI and CLI. Settings will not be upgraded from previous versions. This applies to all FortiGate models.

To ensure uninterrupted remote access, customers must migrate their SSL VPN tunnel mode configuration to IPsec VPN before upgrading to FortiOS 7.6.3 and later.

See [Migration from SSL VPN tunnel mode to IPsec VPN](#) in the *FortiOS 7.6 New Feature* guide for detailed steps on migrating to IPsec VPN before upgrade.

A complete migration guide can be found in the following links:

- For FortiOS 7.6, see [SSL VPN to IPsec VPN Migration](#).
- For FortiOS 7.4, see [SSL VPN to IPsec VPN Migration](#).

## Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models

On the following FortiGate models, the Agentless VPN (formerly SSL VPN web mode) feature is no longer available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-50G/FWF-50G and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)
- FGT-70G/FWF-70G and variants
- FGT-90G and FGT-91G

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).

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See [SSL VPN to IPsec VPN Migration](#) for more information.



FortiGate models not listed above will continue to support Agentless VPN (formerly SSL VPN web mode). However, SSL VPN tunnel mode is not longer supported on any models.

---

## 2 GB RAM FortiGate models no longer support most FortiOS proxy-related features

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, FortiOS no longer supports most proxy-related features.

However FortiOS 7.6.5 brings back proxy-based inspection for email protocols on FortiGate models with 2 GB RAM. This covers the following services:

- SMTP(s)
- POP3(s)
- IMAP(s)

- NNTP

Firewall policies can once again support proxy-based inspection mode when users select one or more of the above services in the firewall policy.

This change impacts the FortiGate 40F, 60F, and 50G series devices, along with their variants.

See [Proxy-related features no longer supported on FortiGate 2 GB RAM models](#) for more information.

## 2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology

To enhance the stability of physical FortiGate devices with 2 GB RAM, the Security Rating feature and Security Fabric topology visibility have been removed. These changes prioritize device stability and mitigate potential performance issues. For more information, see [Optimizations for physical FortiGate devices with 2 GB RAM](#).

## GUI access conflict with IPsec TCP tunnel on the same interface

In FortiOS version 7.6.1, the default IKE TCP port has been changed to port 443 on new deployments. In the FortiOS 7.6.1 Release Notes, see Bug ID 1051144 in [Changes in default values](#).

This may affect GUI access for interfaces bound to an IPsec tunnel in the scenario that the GUI admin port is also using port 443.

In case GUI connectivity is lost, connect to the FortiGate by:

1. Connecting from an interface that is not bound to an IPsec tunnel.
2. Connecting to the interface using SSH, if SSH is enabled.
3. Connecting to the FortiGate from console.

To ensure continued functionality, users are recommended to either:

- Choose an alternative interface for GUI access by configuring:

```
config system global
    set admin-sport <port>
end
```

- Customize the `ike-tcp-port` to a value other than 443:

```
config system settings
    set ike-tcp-port <port>
end
```

## SAML certificate verification

For security purposes, in previous versions, FortiGate required a signature verification for both the SAML response message and the SAML assertion carried inside the SAML response. This means that the SAML response must have a valid signature, and the SAML assertion must also have a valid signature. If the Identity Provider (IdP) provides an invalid signature, or fails to sign one of these, the FortiGate will reject the SAML response.

This has now been loosened with the following configuration:

```
config user saml
  edit <name>
    set require-signed-resp-and-asrt <enable | disable>
  next
end
```

| Option  | Description                                                               |
|---------|---------------------------------------------------------------------------|
| enable  | Both response and assertion must be signed and valid.                     |
| disable | At least one of response or assertion must be signed and valid (default). |

By default, the setting is disabled, which only requires one of the response or assertion to be signed and valid.

For more information, see [Identify Providers](#).

## Policy check required for hairpin traffic

In FortiOS 7.6.5, the default setting for `allow-traffic-redirect` and `ipv6-allow-traffic-redirect` changed from enable to disable:

```
config system global
  set allow-traffic-redirect disable
  set ipv6-allow-traffic-redirect disable
end
```

Upon upgrade, both of these settings will be changed to `disable`, even if they were enabled before.

Disabling this setting ensures that hairpin traffic arriving at an interface and redirected out on the same interface requires a firewall policy to explicitly allow the traffic. If you want to redirect traffic without the need for a policy based only on routing decision, then manually enable these settings.

## Changing vlan-lookup-cache requires system restart

Enabling or disabling `vlan-lookup-cache` or any configuration change that causes a system restart can disrupt the operation of an FGCP cluster. If possible, you should make this configuration change to the individual FortiGates before setting up the cluster. If the cluster is already operating, you should temporarily remove the secondary FortiGate(s) from the cluster, change the configuration of the individual FortiGates and then re-form the cluster. You can remove FortiGate(s) from a cluster using the *Remove Device from HA cluster* button on the *System > HA GUI* page. For more information, see [Disconnecting a FortiGate](#).

# Changes in CLI

| Bug ID  | Description                                                                                                                                                                                                                                                                                     |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 895242  | For the FortiGate-6000 and 7000 platforms, the default HA upgrade mode has been changed from simultaneous to uninterruptible.                                                                                                                                                                   |
| 1238936 | The SFP speed detect CLI option has been updated, replacing auto-module with detect-by-module for improved clarity.                                                                                                                                                                             |
| 1266730 | <p>The arp-reply CLI option is now supported for IPv4 and IPv6 firewall VIPs. The arp-reply option is enabled by default and you can use the following command to disable ARP replies for a firewall VIP:</p> <pre>config firewall vip     edit new-vip         set arp-reply disable end</pre> |

# Changes in default behavior

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1207557 | The default behavior has changed: when Anycast is enabled, VM license activation now uses dedicated activation FQDNs (vmactivation1/2/3.fortinet.net) instead of general update FQDNs, resulting in faster and more reliable activation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 1238339 | <ul style="list-style-type: none"><li>• Enable the dedicated host queue by default to carry critical traffic. This secures critical connections like BFD, BGP, LACP, even under extreme background load.</li><li>• NP7 DSWH profile change to improve the buffer performance</li><li>• Don't return e_busy at the NP7 driver to prevent CPU exhaustion under intense retry</li><li>• Enable the dedicated-management-cpu by default to prevent regular traffic from running on CPU0, which is also used for processing critical traffic on lower-end NP7 platforms.<br/>* To maximize the CPS performance, you may disable this feature.</li><li>• Regular host queues now drop packets at DSWH under extreme load, instead of doing backpressure to DSW. This helps to show which CPU core is busy during debugging and prevents bigger issues, such as CG_FULL.</li></ul> |
| 1239371 | <p>FortiGate operating in GovRamp (previously called StateRAMP) mode will use dedicated FortiGuard NTP servers as the default configuration after a factory reset.</p> <p><b>Previous Behavior</b></p> <p>After a factory reset in GovRamp mode, FortiGate defaulted to the following custom NTP servers:</p> <pre>time-a-g.nist.gov   129.6.15.28 time-b-g.nist.gov   129.6.15.29</pre> <p><b>New Default Behavior</b></p> <p>Following a factory reset, the system now defaults to dedicated FortiGuard NTP servers:</p> <pre>ntp1.fortinetgov.com   23.249.63.60/23.249.63.61 ntp2.fortinetgov.com   23.249.63.62/23.249.63.63</pre>                                                                                                                                                                                                                                     |
| 1240706 | In NGFW policy-based mode, traffic may be bypassed when the IPS engine is not running such as when FortiGate first boots up, the IPS engine is upgrading or when it is manually stopped with debug commands. Instead, NGFW policy mode VDOMs will now drop traffic when IPS sockets are not available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1245249 | <p>Additional commands are allowed before device registration to accommodate users that require configuring the device for central management, ZTP and LTP.</p> <p>Commands added:</p> <ul style="list-style-type: none"><li>• config firewall policy</li><li>• config router setting</li><li>• config router static</li><li>• config router static6</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <ul style="list-style-type: none"><li>• config system admin</li><li>• config system central-management</li><li>• config system dns</li><li>• config system interface</li><li>• config system pppoe-interface</li><li>• config system settings</li></ul>                                                                                                                                                                                                                                                                                 |
| 1256231 | <p>The CLI prompt includes the device HA role (Primary/Secondary). This dynamic labeling updates automatically following failover events but changes the prompt format, which can impact automation scripts (for example, Ansible) that rely on fixed prompt patterns.</p> <p>New CLI:</p> <pre>FortiGate(Secondary) (global) # get system status Version: FortiGate-3000F v7.6.7,build3704,260601 (GA.M)</pre> <p>Old CLI:</p> <pre>FortiGate (global) # get system status Version: FortiGate-3000F v7.6.6,build3652,260127 (GA.</pre> |
| 1288059 | <p>On FortiGate 20xG models, port1 and port2 are removed from the virtual switch and configured for DHCP by default after a factory reset or out-of-box initialization to support Zero Touch Provisioning (ZTP) over these ports.</p>                                                                                                                                                                                                                                                                                                   |

# Changes in default values

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1248524 | <p>The default MTU for IPsec tunnel interfaces has been changed from 1420 to 1402 on the following FortiGate models:</p> <p>FG-5xG, FG-7xG, FG-9xG, FG-12xG, FG-20xG, FG-40xF, FG-60xF, FG-70xG, FG-90xG, FG-100xF, FG-180xF, FG-260xF, FG-300xF, FG-320xF, FG-350xF, FG-370xF, FG-420xF, FG-440xF, FG-480xF, FG-7000F, FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-ARM64-XEN, FG-VM64, FG-VM64-ALI, FG-VM64-AZURE, FG-VM64-AWS, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-XEN, FG-VM64-KVM, FG-VM64-OPC.</p> |

# Changes in table size

| Bug ID  | Description                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------------------|
| 1132879 | Increase extension-controller.extender size for FGT-200G and higher end to 512 to support more lan-extension connections. |

# New features or enhancements

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

## FortiASIC

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1192303    | <p>On FortiGates with NP7 processors, the following new option is available to enable or disable VLAN accounting:</p> <pre>config system npu     set vlan-accounting {disable   enable} end</pre> <p>VLAN accounting is enabled by default.</p> <p>VLAN accounting on a busy FortiGate with a large number of VLANs can generate large numbers of VLAN lookup (SPV/TPV) messages. In some cases these messages can cause CG-FULL conditions or packet drops, especially on very busy systems.</p> <p>You can use the following command to reduce the number of VLAN accounting messages that are generated by increasing the VLAN accounting interval.</p> <pre>config system npu     set vlan-acct-interval &lt;milliseconds&gt; end</pre> <p>The default VLAN accounting interval is 200 milliseconds. The range is 100 to 10000 milliseconds.</p> |
| 1205727    | <p>You may be able to reduce FGCP HA failover times by changing the the NP7 link scan interval. The NP7 link scan interval is the amount of time that a FortiGate with NP7 processors waits between scans to determine if a link has failed. A shorter NP7 link scan interval can cause the FortiGate to send gratuitous ARP packets sooner after an HA failover has occurred.</p> <pre>config system npu     set np-linkscan-interval &lt;milliseconds&gt; end</pre> <p>The np-link-scan-interval range is 50 to 1000ms. The default NP7 link scan interval is 1000 milliseconds (ms). If your FGCP HA cluster experiences longer than expected HA failover delays (for example a 2-second interval for a failover to occur), reducing the NP7 link scan interval may reduce HA failover delays.</p>                                                |

| Feature ID | Description                                                                                                                                                                               |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1288373    | Introduces NPU offload support for IPsec over VNE interfaces on SoC5/NP7Lite and NP7 platforms, enabling hardware acceleration at the driver level, improving performance and throughput. |

## GUI

See [GUI](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                        |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1176612    | A new "Legal Third Party" panel has been added to the FortiOS GUI, providing a searchable and exportable list of all third-party software used in the product, along with their required licenses, license terms, and version information. This enhancement centralizes all third-party licensing details in a single, easily accessible location. |
| 1260021    | During the 7-day setup period, administrators can upgrade or downgrade the device manually through GUI and CLI. After the 7-day setup period, administrators must register to perform upgrade and downgrade.                                                                                                                                       |

## Hyperscale

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1212583    | <p>On FortiGateS licensed for Hyperscale firewall, the following new options are available to improve control over timers related to Endpoint Independent filtering (EIF) sessions. EIF is also called full-cone NAT.</p> <pre>config system npu     set eif-tcp-refresh-dir {both   outgoing   incoming}     set eif-udp-refresh-dir {both   outgoing   incoming}     set eif-tcp-ttl &lt;time&gt;     set eif-udp-ttl &lt;time&gt;     set extra-timeout-tcp &lt;time&gt;     set extra-timeout-udp &lt;time&gt; end</pre> |
| 1220140    | <p>If your hyperscale firewall users are authenticated using RSO, and you have configured hyperscale hardware logging to include user information in hardware log messages, you can now include the RADIUS server prefix length in the log server group configuration:</p> <pre>config log npu-server</pre>                                                                                                                                                                                                                  |

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <pre> set log-processor host config server-group   edit &lt;group-name&gt;     set log-mode {per-session   per-nat-mapping   per-session-ending}     set log-format syslog     set log-user-info enable     set rso-ipv6-prefix-length &lt;length&gt;     set rso-ipv4-prefix-length &lt;length&gt;   next end next end </pre> <p>The default &lt;length&gt; (64 for IPv6 and 32 for IPv4) works with most RADIUS servers.</p> |

## LAN Edge

See [LAN Edge](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                            |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1197063    | Add support for channels 1 through 93 in the 6 GHz range for all G and K platforms for the Ukraine-U region.                                                                                                                                                                                                           |
| 1238935    | Adds support for defining trunk portselection criteria at the global switchcontroller level on Marvell platforms. Centralizing this configuration replaces the previous pertrunk approach.                                                                                                                             |
| 1244920    | Adds the ability to enable both Dynamic VLAN and VLAN Pooling simultaneously when configuring a VAP with RADIUS authentication. This enhancement expands flexibility in enterprise deployments by allowing VLAN assignment from RADIUS or, when absent, falling back to the local VLAN pool for seamless segmentation. |
| 1244925    | Enhances VLAN pooling in WTP group mode by allowing multiple WTP groups to be selected when creating a VLAN entry. This improves flexibility and scalability for environments where VLAN pools must span several WTP groups.                                                                                           |
| 1249992    | Enables MultiLink Operation (MLO) on Local Standalone VAPs for FortiAPK models, extending WiFi 7 MLO capabilities beyond Managed FortiAPs. Authentication is handled directly on the FortiAP, allowing full MLO functionality even when operating independently.                                                       |

## Network

See [Network](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                                                             |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1215201    | Adds support for an external active GNSS antenna on FWF50G5G, extending the existing GPS feature to enable stronger signal reception. This enhancement improves GPS accuracy and reliability in environments where the built-in passive antenna is insufficient.                                                                                                                        |
| 1215886    | <p>Add a new setting that functions like strict Reverse Path Forwarding checks for reply packets.</p> <pre>config system settings   set src-check-reply {enable   disable} end</pre> <p>Where:</p> <ul style="list-style-type: none"><li>• enable: Enable source verification for reply packets.</li><li>• disable: Disable source verification for reply packets (default)."</li></ul> |

## Policy & Objects

See [Policy and objects](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                           |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1105204    | Adds support for using SCIM groups directly in firewall policies, eliminating the need for local group mapping, simplifying identity-based access control. Additionally enables IPsec VPN authorization by matching certificate SAN fields with SCIM user attributes, ensuring consistent and streamlined user authentication and policy enforcement. |

## Security Fabric

See [Security Fabric](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1250003    | Introduces a new default automation stitch (Firmware Upgrade Complete), a new automation trigger (Auto Firmware Upgrade Complete), and a new automation action (Auto Upgrade Complete Email Notification); additionally, the firmwareupgrade email notification has been improved for greater clarity, and the previous default automation stitch (Firmware Upgrade Notification) has been disabled. |

## Security Profiles

See [Security profiles](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1199124    | Adds WebSocket traffic inspection, allowing UTM modules including DLP, AV, IPS and FileFilter to detect and block sensitive data, malware, and restricted files sent over WebSocket. With the growing adoption of WebSocket-based applications, this provides essential security coverage previously unavailable. |

## System

See [System](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1223803    | Introducing customizable DHCP Option 82 configuration, enabling administrators to select any combination of suboptions and define a custom delimiter. It replaces the previous configuration of only three fixed, noneditable styles.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 1238520    | To facilitate use cases where a FortiGate device needs to be configured before being sent to end-users, models that require registration before full GUI and CLI access now have a 7-day setup period for full configurations before registration becomes a requirement.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 1254298    | Adds GUI support for monitoring 5G modem status and performing firmware upgrades, improving visibility and streamlining maintenance workflows.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 1256067    | The FortiGate FortiGuard communication protocol (FCPC) is enhanced to accept a new ForcedUpdate flag as well as the major.minor.patch-build versioning from the FortiGate. When a FortiGate observes its firmware license is invalid, it will send FortiGuard a firmware upgrade message with the ForcedUpdate flag and its versioning. In turn, FortiGuard server will ignore license check for that device and parse its firmware version. If the major and minor version on the upgrade-from and upgrade-to firmware are the same, the upgrade will be allowed. Furthermore logs, notifications and automation stitches are improved to provide clearer indication of auto-upgrade and required-upgrade within its messaging. |
| 1256231    | Enhances the CLI prompt to include the device HA role (Primary/Secondary), improving immediate role visibility. This dynamic labeling updates automatically following failover events but changes the prompt format, which can impact automation scripts (for example, Ansible) that rely on fixed prompt patterns.                                                                                                                                                                                                                                                                                                                                                                                                              |
| 1256235    | Adds support for preserving permember SNMP system information, including location, description, and contact information. This allows administrators to uniquely identify and manage each HA unit in SNMP monitoring tools, even when members are deployed across different sites.                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Feature ID | Description                                                                                                                                                        |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1274821    | Adds support for Connectivity Fault Management (CFM) on FortiGate Gseries platforms, enabling administrators to diagnose and troubleshoot Ethernet network issues. |

## VPN

See [IPsec and SSL VPN](#) or [Agentless VPN](#) in the New Features Guide for more information.

| Feature ID | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1212772    | By default, changes to outbandwidth or egress shaping profiles on a physical or VLAN interface do not take effect for IPsec tunnels or sessions that are already established and offloaded by NP7 or NP7Lite (SOC5) processors. To apply the updated egress shaping settings, you must flush or reinstall the affected IPsec SAs and clear any offloaded sessions. Doing this rebuilds the IPsec tunnel and associated sessions using the new interface shaping configuration. For FortiGates with NP7Lite (SOC5) processors, you can use the following command to cause FortiOS to automatically flush or reinstall the affected IPsec SAs and clear any offloaded sessions after changing the configuration of an outbandwidth or egress shaping profile: <code>config system npu set mcs-auto-start enable end mcs-auto-start</code> is disabled by default." |
| 1212920    | Native VPN remote access configurations have been improved on the VPN wizard. For supported OS's, configurations from the VPN wizard will work out of the box. Native VPN client defaults to using L2TP over IPsec for Windows, Android and macOS/iOS clients. Admins can also configure IKEv2 for Windows and Android clients.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 1235059    | IPsec multipath allows encrypted tunnel traffic to be distributed across multiple sub-tunnels and CPU queues simultaneously. By grouping these sub-tunnels into a single logical super tunnel, FortiGate can utilize multiple CPU cores in parallel, significantly increasing VPN throughput without requiring changes to the overall tunnel design or addressing plan.<br>To enable:<br><br><pre>config vpn ipsec phase1-interface   edit &lt;name&gt;     set multipath &lt;integer&gt;   next end</pre>                                                                                                                                                                                                                                                                                                                                                       |
| 1262907    | Allow unaddressed IPsec tunnel interfaces to be used as PIM interfaces by borrowing the IP address of a loopback interface.<br><br><pre>config router multicast   config interface     edit "p1"       set update-source "lo1"     next   end end</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## ZTNA

See [Zero Trust Network Access](#) in the New Features Guide for more information.

| FeatureID | Description                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1206912   | <p>Add a new option for secure webproxy clients to opt-out from using EMS CA certificate.</p> <pre>config authentication setting     set ems-root-ca {enable*   disable} end</pre> <p>Enable/disable use of the EMS root CA for FortiClient, ZTNA, and endpoint authentication (default = enable).</p> <p>When disabled, WAD checks client cert based on the user CA setup.</p> |

# Upgrade information

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

| FortiGate                                                | Upgrade option                                                         | Details                                                                                                                                        |
|----------------------------------------------------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Individual FortiGate devices                             | Manual update                                                          | Use the procedure in this topic. See also <a href="#">Upgrading individual devices</a> in the FortiOS Administration Guide.                    |
|                                                          | Automatic update based on FortiGuard upgrade path                      | See <a href="#">Enabling automatic firmware updates</a> in the FortiOS Administration Guide for details                                        |
| Multiple FortiGate devices in a Fortinet Security Fabric | Manual, immediate or scheduled update based on FortiGuard upgrade path | See <a href="#">Fortinet Security Fabric upgrade on page 30</a> and <a href="#">Upgrading all devices</a> in the FortiOS Administration Guide. |

## To view supported upgrade path information:

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

## Fortinet Security Fabric upgrade

FortiOS 7.6.7 is verified to work with these Fortinet products. This includes:

|                                           |                              |
|-------------------------------------------|------------------------------|
| <b>FortiAnalyzer</b>                      | • 7.6.7                      |
| <b>FortiManager</b>                       | • 7.6.7                      |
| <b>FortiExtender</b>                      | • 7.4.0 and later            |
| <b>FortiSwitch OS (FortiLink support)</b> | • 6.4.6 build 0470 and later |

|                                      |                                                                                                         |
|--------------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>FortiAP</b>                       | • 7.2.2 and later                                                                                       |
| <b>FortiAP-U</b>                     | • 6.2.5 and later                                                                                       |
| <b>FortiAP-W2</b>                    | • 7.2.2 and later                                                                                       |
| <b>FortiClient EMS</b>               | • 7.0.3 build 0229 and later                                                                            |
| <b>FortiClient Microsoft Windows</b> | • 7.0.3 build 0193 and later                                                                            |
| <b>FortiClient Mac OS X</b>          | • 7.0.3 build 0131 and later                                                                            |
| <b>FortiClient Linux</b>             | • 7.0.3 build 0137 and later                                                                            |
| <b>FortiClient iOS</b>               | • 7.0.2 build 0036 and later                                                                            |
| <b>FortiClient Android</b>           | • 7.0.2 build 0031 and later                                                                            |
| <b>FortiSandbox</b>                  | • 2.3.3 and later for post-transfer scanning<br>• 4.2.0 and later for post-transfer and inline scanning |

\* If you are using FortiClient only for IPsec VPN, 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 7.6.0, use FortiClient 7.6.0.

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

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiExtender devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.6.7. When Security Fabric is enabled in FortiOS 7.6.7, all FortiGate devices must be running FortiOS 7.6.7.

---

## 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*.

## 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 7.6.7:

1. Use the following command to set the upgrade-mode to uninterruptible to support HA graceful upgrade:

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



When upgrading from FortiOS 7.4.1 to a later version, use the following command to enable uninterruptible upgrade:

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

2. Download the FortiOS 7.6.7 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. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

## Default setting of cp-accel-mode is changed to none on 2GB memory models

This change disables CP acceleration to lower system memory usage thus can prevent some unexpected behavior due to lack of memory.

Previous FortiOS CLI behavior:

```
config ips global
    set cp-accel-mode advanced
end
```

New FortiOS CLI behavior after upgrade:

```
config ips global
    set cp-accel-mode none
end
```

This change will cause performance impact as CPU will do the pre-match (pattern match) inside IPS (CPU) instead of hardware engine (cp module in SOC4). Some customers could expect an increase in CPU utilization as a result.

FortiGate and FortiWiFi 4xF/6xF families are affected by this change.

## Policies that use an interface show missing or empty values after an upgrade

If local-in policy, DoS policy, interface policy, multicast policy, TTL policy, or central SNAT map used an interface in version 7.4.5, 7.6.0 GA or any previous GA version that was part of the SD-WAN zone, these policies will be deleted or show empty values after upgrading to version 7.4.6 or 7.6.1 or later.

This issue is resolved in FortiOS 7.6.3 with mantis 1104649.

After following the upgrade path to FortiOS 7.6.3, you must manually recreate these policies and assign them to the appropriate SD-WAN zone.



Although not recommended, you can skip the upgrade path and upgrade directly to FortiOS 7.6.3, and the policies remain untouched. Skipping upgrade steps might cause devices to miss other important FortiOS checks and changes and is not recommended.

---

## Managed FortiSwitch do not permit empty passwords for administrator accounts

Starting from FortiOS version 7.6.1, a managed FortiSwitch no longer permits empty passwords for the admin account. If a FortiSwitch unit was previously authorized without an admin password, the FortiGate will automatically generate a random admin password for the FortiSwitch upon upgrading to 7.6.1 or later. This change will cause the admin to lose access.

To regain access, configure a password override on the FortiGate device using the following commands:

```
config switch-controller switch-profile
    edit default
        set login-passwd-override enable
        set login-passwd <passwd>
    next
end
```



FortiSwitch units with an existing admin password will not be affected by this change.

---

## Removed speed setting affects SFP+ interfaces after upgrade

Due to `1000auto` speed setting removal on FortiGate 1000F/1001F in FortiOS 7.6.1, upgrade from previous version may result in interface down because speed setting changed to `10000full` on SFP+ interface, which previously used speed `1000auto`. Administrators may need to manually change speed setting to `1000full` to restore the connection.

## Hyperscale with FGCP HA clusters and interface monitoring

For previous versions of hyperscale FortiOS, FGCP HA clustering with hardware session synchronization with `config vcluster-status disabled` allowed you to monitor `hw-session-sync-dev` interfaces. FortiOS 7.6.3 changed this behavior, and you can no longer monitor `hw-session-sync-dev` interfaces.

If your HA configuration includes monitoring `hw-session-sync-dev` interfaces, the upgrade to FortiOS 7.6.4 removes the monitor interface configuration.

You can work around this problem by removing monitoring from `hw-session-sync-dev` interfaces or by selecting different interfaces to be `hw-session-sync-dev` interfaces before performing the upgrade.

## Password policy enforcement

After upgrade to FortiOS 7.6.5 or later, the password policy is enforced, and your password must meet the requirements before you can log in to FortiOS. Passwords must contain:

- 1 uppercase letter
- 1 lowercase letter
- 1 special character
- 1 number (0-9)
- A minimum length of 12 characters

If your password meets the requirements, you can log in to FortiOS after upgrade.

If your password does not meet the requirements, you must change your password before you can log in to the GUI or CLI.

# Product integration and support

The following table lists FortiOS 7.6.7 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 135</li><li>• Mozilla Firefox version 138</li><li>• Google Chrome version 136</li></ul> <p>Other browser versions have not been tested, but may fully function.<br/>Other web browsers may function correctly, but are not supported by Fortinet.</p>                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Explicit web proxy browser</b>     | <ul style="list-style-type: none"><li>• Microsoft Edge 135</li><li>• Mozilla Firefox version 138</li><li>• Google Chrome version 136</li></ul> <p>Other browser versions have not been tested, but may fully function.<br/>Other web browsers may function correctly, but are not supported by Fortinet.</p>                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>FortiController</b>                | <ul style="list-style-type: none"><li>• 5.2.5 and later</li></ul> <p>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Fortinet Single Sign-On (FSSO)</b> | <ul style="list-style-type: none"><li>• 5.0 build 0333 and later (needed for FSSO agent support OU in group filters)</li><li>• Windows Server 2025 Standard</li><li>• Windows Server 2025 Datacenter</li><li>• Windows Server 2025 Core</li><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>• Novell eDirectory 8.8</li></ul> |
| <b>AV Engine</b>                      | <ul style="list-style-type: none"><li>• 7.00054</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>IPS Engine</b>                     | <ul style="list-style-type: none"><li>• 7.01187</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

See also:

- [Virtualization environments on page 38](#)
- [Language support on page 38](#)
- [Agentless VPN support on page 39](#)
- [FortiExtender modem firmware compatibility on page 39](#)

## Virtualization environments

The following table lists hypervisors and recommended versions.

| Hypervisor                      | Recommended versions                                                                                                                                                           |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Citrix Hypervisor</b>        | <ul style="list-style-type: none"><li>• 8.2 Express Edition, CU1</li></ul>                                                                                                     |
| <b>Linux KVM</b>                | <ul style="list-style-type: none"><li>• Ubuntu 22.04.3 LTS</li><li>• Red Hat Enterprise Linux release 9.4</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>• Windows Server 2022</li></ul>                                                                                                          |
| <b>Windows Hyper-V Server</b>   | <ul style="list-style-type: none"><li>• Microsoft Hyper-V Server 2022</li></ul>                                                                                                |
| <b>Open source XenServer</b>    | <ul style="list-style-type: none"><li>• Version 3.4.3</li><li>• Version 4.1 and later</li></ul>                                                                                |
| <b>VMware ESXi</b>              | <ul style="list-style-type: none"><li>• Versions 6.5, 6.7, 7.0, 8.0, and 9.0.</li></ul>                                                                                        |

## Language support

The following table lists language support information.

### Language support

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

| Language            | GUI |
|---------------------|-----|
| Portuguese (Brazil) | ✓   |
| Spanish             | ✓   |

## Agentless VPN support

The following table lists the operating systems and web browsers supported by Agentless VPN (formerly SSL VPN web mode). See also [SSL VPN tunnel mode replaced with IPsec VPN on page 13](#).

| Operating System                          | Web Browser                                                                         |
|-------------------------------------------|-------------------------------------------------------------------------------------|
| Microsoft Windows 7 SP1 (32-bit & 64-bit) | Mozilla Firefox version 138<br>Google Chrome version 136                            |
| Microsoft Windows 10 (64-bit)             | Microsoft Edge 135<br>Mozilla Firefox version 138<br>Google Chrome version 136      |
| Ubuntu 20.04 (64-bit)                     | Mozilla Firefox version 138<br>Google Chrome version 136                            |
| macOS Ventura 13.1                        | Apple Safari version 18<br>Mozilla Firefox version 137<br>Google Chrome version 136 |
| iOS                                       | Apple Safari<br>Mozilla Firefox<br>Google Chrome                                    |
| Android                                   | Mozilla Firefox<br>Google Chrome                                                    |

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

## FortiExtender modem firmware compatibility

The following table lists the modem firmware file name and version for each FortiExtender model and its compatible geographical region.

| FortiExtender model | Modem firmware image name    | Modem firmware file on Support site        | Geographical region |
|---------------------|------------------------------|--------------------------------------------|---------------------|
| FEX-101F-AM         | FEM_EM06A-22-1-1             | FEM_EM06A-22.1.1-build0001.out             | America             |
| FEX-101F-EA         | FEM_EM06E-22-01-01           | FEM_EM06E-22.1.1-build0001.out             | EU                  |
|                     | FEM_EM06E-22.2.2             | FEM_EM06E-22.2.2-build0002.out             | EU                  |
| FEX-201E            | FEM_06-19-0-0-AMEU           | FEM_06-19.0.0-build0000-AMEU.out           | America and EU      |
|                     | FEM_06-19-1-0-AMEU           | FEM_06-19.1.0-build0001-AMEU.out           | America and EU      |
|                     | FEM_06-22-1-1-AMEU           | FEM_06-22.1.1-build0001-AMEU.out           | America and EU      |
|                     | FEM_06-22-1-2-AMEU           | FEM_06-22.1.2-build0001-AMEU.out           | America and EU      |
| FEX-201F-AM         | FEM_07A-22-1-0-AMERICA       | FEM_07A-22.1.0-build0001-AMERICA.out       | America             |
|                     | FEM_07A-22-2-0-AMERICA       | FEM_07A-22.2.0-build0002-AMERICA.out       | America             |
| FEX-201F-EA         | FEM_07E-22-0-0-WRLD          | FEM_07E-22.0.0-build0001-WRLD.out          | World               |
|                     | FEM_07E-22-1-1-WRLD          | FEM_07E-22.1.1-build0001-WRLD.out          | World               |
| FEX-202F-AM         | FEM_07A-22-1-0-AMERICA       | FEM_07A-22.1.0-build0001-AMERICA.out       | America             |
|                     | FEM_07A-22-2-0-AMERICA       | FEM_07A-22.2.0-build0002-AMERICA.out       | America             |
| FEX-202F-EA         | FEM_07E-22-1-1-WRLD          | FEM_07E-22.1.1-build0001-WRLD.out          | World               |
| FEX-211E            | FEM_12-19-1-0-WRLD           | FEM_12-19.1.0-build0001-WRLD.out           | World               |
|                     | FEM_12-19-2-0-WRLD           | FEM_12-19.2.0-build0002-WRLD.out           | World               |
|                     | FEM_12-22-1-0-AMEU           | FEM_12-22.0.0-build0001-AMEU.out           | America and EU      |
|                     | FEM_12-22-1-1-WRLD           | FEM_12-22.1.1-build0001-WRLD.out           | World               |
| FEV-211F_AM         | FEM_12_EM7511-22-1-2-AMERICA | FEM_12_EM7511-22.1.2-build0001-AMERICA.out | America             |

| FortiExtender model | Modem firmware image name    | Modem firmware file on Support site        | Geographical region |
|---------------------|------------------------------|--------------------------------------------|---------------------|
| FEV-211F            | FEM_12-22-1-0-AMEU           | FEM_12-22.1.0-build0001-AMEU.out           | World               |
| FEX-211F-AM         | FEM_12_EM7511-22-1-2-AMERICA | FEM_12_EM7511-22.1.2-build0001-AMERICA.out | America             |
| FEX-212F            | FEM_12-19-2-0-WRLD           | FEM_12-19.2.0-build0002-WRLD.out           | World               |
|                     | FEM_12-22-1-1-WRLD           | FEM_12-22.1.1-build0001-WRLD.out           | World               |
| FEX-311F            | FEM_EM160-22-02-03           | FEM_EM160-22.2.3-build0001.out             | World               |
|                     | FEM_EM160-22-1-2             | FEM_EM160-22.1.2-build0001.out             | World               |
| FEX-511F            | FEM_RM502Q-21-2-2            | FEM_RM502Q-21.2.2-build0003.out            | World               |
|                     | FEM_RM502Q-22-03-03          | FEM_RM502Q-22.3.3-build0004.out            | World               |
|                     | FEM_RM502Q-22-04-04-AU       | FEM_RM502Q-22.4.4-build0005_AU.out         | Australia           |
|                     | FEM_RM502Q-22-1-1            | FEM_RM502Q-22.1.1-build0001.out            | World               |
|                     | FEM_RM502Q-22-2-2            | FEM_RM502Q-22.2.2-build0002.out            | World               |

The modem firmware can also be uploaded manually by downloading the file from the Fortinet Customer Service & Support site. The firmware file names are listed in the third column of the table.

#### To download the modem firmware:

1. Go to <https://support.fortinet.com/Download/FirmwareImages.aspx>.
2. From the *Select Product* dropdown, select *FortiExtender*.
3. Select the *Download* tab.
4. Click *MODEM-Firmware*.
5. Select the FortiExtender model and image name, then download the firmware file.

# Resolved issues

The following issues have been fixed in version 7.6.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

## Agentless VPN

| Bug ID  | Description                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------|
| 1203158 | An error condition occurs when the maximum number of concurrent users is reached                                                  |
| 1214345 | High memory usage occurs when multiple VDOMs are configured with SSLVPN.                                                          |
| 1216477 | Blocked IP addresses are cleared when login-block-time is not reached in multiple VDOMs with different login-block-time settings. |
| 1234918 | Insecure Content-Security-Policy occurs when SSL VPN portal is accessed                                                           |
| 1240901 | PCI scan fails when using HTTP/1.0 on the SSLVPN port                                                                             |
| 1247129 | Browser offers to save RDP credentials when Agentless VPN is configured                                                           |
| 1257802 | RDP disconnections occur when high monitor refresh rate triggers command limit in Agentless VPN web portal                        |
| 1272207 | Authentication failure occurs when username and OTP are concatenated during SSLVPN login on FortiOS 7.4.11                        |

## AntiVirus

| Bug ID  | Description                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------|
| 1125299 | HTTP logs are missing HTTP method and agent information when uploading files using HTTP POST/PUT.           |
| 1214247 | When FortiSandbox inline scan is configured in proxy inspection mode, timeout occurs prematurely.           |
| 1249056 | An error condition occurs in the antivirus daemon during database updates.                                  |
| 1260804 | Zip file download is blocked when Antivirus profile is configured in Proxy mode and scanned by stream scan. |
| 1281140 | Fields are missing from Message ID 8195 when using multipart/form-data Content-Type                         |

## Application Control

| Bug ID  | Description                                                                                    |
|---------|------------------------------------------------------------------------------------------------|
| 1156066 | Communication breaks when application control is used in policy over EMAC VLAN interfaces      |
| 1264508 | Application control fails to block small files through WeChat when using proxy inspection mode |

## DNS Filter

| Bug ID  | Description                                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------|
| 1229928 | Traffic is not blocked as expected when DNS response returns NXDOMAIN in flow-based mode                                            |
| 1243152 | Incorrect client and server cookies are returned for cached DNS entries when conditional forwarding with EDNS cookies is configured |
| 1254463 | Traffic drop occurs when using wildcard FQDN objects when a certain pattern of FQDN cannot be resolved by passive learning.         |
| 1254680 | DNS-over-TLS fails when configured on FortiGate 201E with FortiOS 7.4.10                                                            |
| 1255195 | DNS query failure occurs when FortiGate acts as recursive DNS server for long TXT records                                           |

## Endpoint Control

| Bug ID  | Description                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------|
| 1037548 | Internal server error occurs when FortiGate requests over 50 fingerprints/users for the EMS /api/v1/report/fct/client_avatars API |
| 1207648 | Intermittent disconnection of EMS Cloud from FortiGate caused by frequent TPM requests from httpsd                                |
| 1226271 | Memory usage issues caused by EMS endpoint requesting many client avatar entries.                                                 |
| 1239851 | Traffic bypasses policy when SIA assigned IP is not updated with ZTNA tag                                                         |

## Explicit Proxy

| Bug ID  | Description                                                                                                                                        |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1237357 | Proxy rule match issues occur when host-regex address values exceed 40 characters                                                                  |
| 1240208 | Intermittent 504 Gateway Timeout errors occur when using explicit proxy after upgrade due to wildcard FQDN not resolving a certain pattern of FQDN |
| 1247518 | HTTP 303 Redirect Loop occurs when accessing websites with SWG SSO connection                                                                      |
| 1252739 | Total shared user count exceeds limit when proxy-auth-lifetime is enabled                                                                          |
| 1257127 | Unexpected behavior in explicit proxy occurs when video filter is enabled and there are multiple requests to the same video ID                     |
| 1281206 | Captive portal fails to appear when IPS is enabled on the proxy policy                                                                             |

## File Filter

| Bug ID  | Description                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------|
| 1186664 | Outlook web client doesn't update emails automatically when proxy-based file-filter is enabled on proxy policy |
| 1208793 | When File Filter is enabled on a proxy policy, some API calls are blocked                                      |

## Firewall

| Bug ID  | Description                                                                                                                                                                                              |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1099748 | HPE incorrectly identifies TCP RST ACK packets as TCP type when receiving RST ACK packets.                                                                                                               |
| 1104208 | NAT is not correctly applied to traffic when a single SYN packet is sent to a VIP without an acknowledgment or reset.                                                                                    |
| 1198219 | Packets are dropped when using auto-asic-offload with EMAC-VLAN over LACP on FortiGate                                                                                                                   |
| 1203504 | Traffic fails over emac-vlan interface between vdoms when offloading is enabled                                                                                                                          |
| 1212772 | Traffic shaping statistics are unavailable when using SOC5                                                                                                                                               |
| 1214413 | The handling of "firewall-session-dirty check-all" has been optimized so that changes to interfaces or policies unrelated to the offloaded session will not cause the offloaded session to become dirty. |

| Bug ID  | Description                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1215851 | Packets are sent back on the same trunk interface when emac-vlan is removed in an emac over LAG setup                                                                                                       |
| 1215886 | Spoofed reply packets bypass FortiGate when strict check is enabled and reply traffic comes from a different interface.                                                                                     |
| 1217157 | GeoIP allow/block functionality fails when configuring VIP with GeoIP as source due to a limitation in number of unique countries (256) that can be added to kernel from a firewall policy.                 |
| 1218523 | ICMP packet drops occur when hardware offloading is enabled                                                                                                                                                 |
| 1230854 | Security exempt list with wildcard FQDN cannot be applied on a captive-portal SSID.                                                                                                                         |
| 1233342 | Traffic drop occurs when ipv4-proto-err is enabled on NP7-based FortiGate                                                                                                                                   |
| 1235349 | Destination IP addresses become unreachable when auto-asic-offload is enabled on the policy where emac-vlan interfaces are used and VRRP virtual mac is enabled                                             |
| 1240706 | In NGFW policy-based mode, traffic may be bypassed when the IPS engine is not running such as when FortiGate first boots up, the IPS engine is upgrading or when it is manually stopped with debug commands |
| 1244717 | Traffic impact occurs when asic-offload is enabled on NP7 over a one-arm EMAC VLAN interface                                                                                                                |
| 1252751 | Virtual servers with custom SSL ciphers are deleted during upgrade                                                                                                                                          |
| 1257907 | NTurbo offload fails when using inter-VDOM links on FortiGate.                                                                                                                                              |
| 1259241 | FortiGate forwards packets with incorrect destination MAC addresses when using EMAC interface with VLAN ID                                                                                                  |
| 1266899 | Traffic disruption occurs when switching NPU's default-qos-type to shaping using QTM module                                                                                                                 |
| 1270494 | Egress shaping-profile cannot accurately limit maximum-bandwidth on VLAN interface when configured on its parent interface on SoC5 models.                                                                  |
| 1271340 | L2TPv3 packets are discarded when protocol 115 is not included as a known protocol on FortiGate                                                                                                             |
| 1274475 | Fragmented packets are forwarded to different LAG member ports when LAG hashing uses both L3 and L4 fields.                                                                                                 |
| 1277509 | Unexpected behavior related to the QTM module when egress-shaping-profile is configured on the parent interface of a VLAN interface.                                                                        |
| 1281193 | FTP passive mode fails when FortiGate is not performing NAT after firmware upgrade from 7.4.9 to 7.6.6                                                                                                      |
| 1286715 | After a firewall address is renamed, duplicate addresses can be accepted in a firewall policy without errors from the CLI.                                                                                  |

## FortiGate 6000/7000 Platform

| Bug ID  | Description                                                                                                                            |
|---------|----------------------------------------------------------------------------------------------------------------------------------------|
| 895242  | 7KF/v7.4.0/b2314: The default setting "uninterruptible-upgrade" is different between SLBC and regular FortiGate platforms              |
| 947982  | Audio cutouts occur when CG_FULL errors are high on NP7 models                                                                         |
| 1170210 | FortiGate Wireless controller Wifi client cannot ping GW/FGT interface. Pass through traffic works fine                                |
| 1179530 | Create session response is dropped when PGW replies with Context Not Found and TEID is null.                                           |
| 1185009 | Traffic on VLAN interfaces is dropped when changing LAG members in emac over VLAN setups due to MAC address changes not being updated. |
| 1231901 | Link-speed test failure occurs when CP10 is configured as Gen4x2                                                                       |
| 1242828 | Erroneous memory allocation may occur under specific conditions on FIMs and the primary FPM during IPv4 and IPv6 routing operations.   |
| 1244720 | Memory usage issues caused by running v4/v6 routing protocols after upgrade                                                            |
| 1253034 | VLAN interface counters show zero Receive/Transmit Bytes and Packets when fastpath is disabled                                         |
| 1260299 | High CPU utilization occurs when config system npu set lag-out-port-select is enabled                                                  |
| 1272827 | Traffic forwarding fails when FGT7081F Primary FPM does not send GARP to connected switch after HA failover.                           |
| 1274545 | Both nodes respond to ARP requests when the HA table is edited in config sys ha.                                                       |

## GUI

| Bug ID  | Description                                                                                                                                        |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 793029  | Unexpected behavior occurs on some FortiGate models when a FortiClient lacks a required MAC address attribute.                                     |
| 981278  | Devices are not displayed on the OT view page when a large number of devices are detected                                                          |
| 1027218 | The "clients" link on the Diagnostics page of any FAP opens one type of client (any of 2.4GHz, 5GHz, or 6GHz bands) and then becomes unresponsive. |
| 1138400 | GUI accessibility issues occur when FortiGate is configured with a large number of FAPs and left idle for an extended period                       |

| Bug ID  | Description                                                                                                                                                                            |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1145510 | Unexpected behavior in Node.JS occurs when creating IPsec tunnels through the wizard                                                                                                   |
| 1165258 | Address group search results are not returned when there are thousands of firewall addresses and groups.                                                                               |
| 1189250 | Upgrade page display issue occurs when HA cluster is in secondary-only mode                                                                                                            |
| 1191076 | Interface bandwidth data is not displayed when LAG is upgraded from 2x40G to 2x100G ports                                                                                              |
| 1194766 | Search functionality issue occurs when viewing threat feed entries from the GUI.                                                                                                       |
| 1196284 | SecurityFabric tooltip displays Client IP when device is detected as a router                                                                                                          |
| 1203957 | Inconsistent license expiration dates appear when viewing license information                                                                                                          |
| 1210579 | An error condition in Node.JS occurs when CSF websocket failure happens on standalone FortiGate.                                                                                       |
| 1214354 | When Security Rating runs a full report on devices that have hundreds of extension devices, device becomes unresponsive when node process CPU and memory utilization suddenly increase |
| 1215246 | Interface deletion fails via GUI on hardware-switch but succeeds on CLI                                                                                                                |
| 1216367 | Access issues occur when admin with custom accprofile logs in to GUI                                                                                                                   |
| 1217015 | Faceplate loading issue occurs when hovering over WAN interface in multi-vdom mode                                                                                                     |
| 1217474 | Unexpected behavior in Node.JS occurs when executing workerpool scripts                                                                                                                |
| 1218901 | GUI widgets display incorrect time when gui-date-time-source is set to system                                                                                                          |
| 1219066 | NAT is enabled automatically when toggling security posture tag in ZTNA policy                                                                                                         |
| 1221215 | Slow GUI performance occurs when searching address groups                                                                                                                              |
| 1224951 | Interface aliases do not display in Performance SLA columns when configured in FortiGate GUI                                                                                           |
| 1228240 | An error condition occurs in the GUI when editing Block/Allow lists under Email Filter                                                                                                 |
| 1228366 | Network interfaces are displayed in incorrect order when accessing Network>Interfaces on FortiGate 30G.                                                                                |
| 1229684 | The FortiGate VM License page is not displayed in the GUI when the FortiGate VM is unlicensed                                                                                          |
| 1230037 | Changes occur when FortiGate is managed by FortiManager and admin logs in with read-only access.                                                                                       |
| 1231087 | Authentication failure occurs when accessing FortiGate through FortiGate Cloud with trusthost configured                                                                               |
| 1233052 | An error condition in Node.JS occurs when token generation fails.                                                                                                                      |
| 1234222 | An error occurs when switching the table from Performance SLAs to SD-WAN Rule                                                                                                          |
| 1234864 | Error condition occurs when checking SIM status Carrier on GUI                                                                                                                         |
| 1235147 | Virtual server clone function becomes edit mode when clicked                                                                                                                           |

| Bug ID  | Description                                                                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1236970 | FortiSM Violation is observed when revision backup on logout is enabled and super_amdin logs out from the GUI                                                         |
| 1237463 | Login failure occurs when post-login-banner is enabled with SAML Single Sign-On                                                                                       |
| 1239075 | Policy dialog page fails to update source object when changing from internet-service to regular address during policy editing                                         |
| 1239337 | User passwords cannot be printed in clear text when logged on with guest admin account                                                                                |
| 1239762 | Config changes are restricted for WiFi when managed by FortiManager for admins with read-write permissions                                                            |
| 1242637 | Firewall policy search issues occur when searching for External Feed objects in a long list                                                                           |
| 1245838 | Incorrect mode option appears for WWAN interface when LTE modem is enabled                                                                                            |
| 1246460 | Incorrect interface information appears when hovering over SFP icon on FGR-70F-3G4G                                                                                   |
| 1247676 | SSH deep scan toggle does not save when enabled on low-end models.                                                                                                    |
| 1248286 | Error occurs when creating a superadmin with two-factor authentication                                                                                                |
| 1249113 | FCT-managed devices with network interfaces connecting to different VDOMs may create multiple interface entries in the user-device-store causing memory usage issues. |
| 1249169 | Incorrect Japanese translation occurs when prompted for one-time upgrade when critical vulnerability detected                                                         |
| 1249302 | An error condition in Node.JS occurs when handling undefined properties.                                                                                              |
| 1251014 | Incorrect interface stats occur when master FIM miscalculates bandwidth and throughput on SLBC platforms                                                              |
| 1252941 | No results appear on the security rating page when logging into the fabric root GUI                                                                                   |
| 1256988 | Brute-force attacks triggered a lot of leaving http_authd processes running and causing memory usage to steadily increase.                                            |
| 1258180 | Display limit in source and destination columns of policy list is increased from 3 to 5 when FortiGate is configured.                                                 |
| 1259193 | An error condition occurs in the login process when accessing the FortiGate and requests for static files are returning HTTP 401                                      |
| 1260292 | Print button is not visible when using prof_admin profile after FortiOS upgrade                                                                                       |
| 1265195 | GUI performance issue occurs when adding or removing members from large firewall address groups                                                                       |
| 1271369 | SAN format options are not available in GUI when creating a CSR on FortiGate                                                                                          |
| 1274070 | File name does not update with CLI console name when renamed                                                                                                          |
| 1277699 | Incorrect display of device and hostname with Korean characters occurs when device detection is enabled and Windows computer name contains Korean characters.         |
| 1291914 | An error condition occurs in the service creation process when using ICMP protocol.                                                                                   |

# HA

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1165361 | CPU usage issues observed during HA led optimization with child process forking                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1205727 | <p>You may be able to reduce FGCP HA failover times by changing the the NP7 link scan interval. The NP7 link scan interval is the amount of time that a FortiGate with NP7 processors waits between scans to determine if a link has failed. A shorter NP7 link scan interval can cause the FortiGate to send gratuitous ARP packets sooner after an HA failover has occurred.</p> <pre>config system npu      set np-linkscan-interval &lt;milliseconds&gt;  end</pre> <p>The np-link-scan-interval range is 50 to 1000ms. The default NP7 link scan interval is 1000 milliseconds (ms). If your FGCPHA cluster experiences longer than expected HA failover delays (for example a 2-second interval for a failover to occur)reducing the NP7 link scan interval may reduce HA failover delays.</p> |
| 1213917 | Interface configuration deletion occurs when QOS is enabled and a reboot happens                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 1214587 | DNS queries are sent from HA reserved management interface when it is configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 1216459 | Verification failure occurs when BIOS security level is set to High during HA image upgrade                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1217228 | Route table deletion occurs when a split brain condition happens in GCP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 1220647 | RX drops occur on HA1 and HA2 ports when upgrading the i40e driver                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 1224835 | Traffic drop occurs when doing HA failover on EMAC VLAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 1225710 | Mobile Token assignment fails on old models that don't support vSN when HA fail-over occurs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1225919 | Packet size issues occur when syncing large FQDN response packets in autoscaling environments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 1226672 | Packet loss occurs when slave member emac-vlan responds to ARP requests in an HA setup with LACP and VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 1231480 | LACPDU transmission issues occur when HA failover is triggered by a monitoring port disconnect                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 1233776 | FSSO user list disappearance occurs when HA failover happens twice.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 1234340 | Asymmetric session handling fails when two FGSP links are configured and only the second link recovers after both go down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 1235313 | Traffic disruption occurs when a large number of firewall policies are installed after a failover during an upgrade in a FortiGate cluster                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 1237317 | No Rx packets occur when unicast-hb is enabled on FortiGate-VM64 with SRIOV.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Bug ID  | Description                                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1240288 | Packets are sent using the cluster MAC address by the secondary cluster member after failover                                                                  |
| 1243380 | Virtual MAC is used by HA-AP Secondary when removing a member from an aggregate interface                                                                      |
| 1244401 | Virtual cluster member dead logs occur when non-primary blades in chassis report HA related logs                                                               |
| 1244800 | An error condition in Confsync occurs when sending large messages through the local socket                                                                     |
| 1244944 | HA heartbeat loss occurs when highest priority is not restricted to heartbeat, routing, and LACP                                                               |
| 1246577 | IPAM is unexpectedly enabled on the HA peer when CSF is enabled or modified.                                                                                   |
| 1248579 | Traffic disruption occurs on EMAC VLAN interfaces during HA failovers                                                                                          |
| 1250174 | Autoscale synchronization issues occur when configuring FortiToken on system admin                                                                             |
| 1250511 | Unexpected Layer 2 bouncing occurs when peer's dev_base is missing in FGSP HA                                                                                  |
| 1260236 | Unexpected power off events occur in FortiGate 70G when configured in HA Active/Passive mode with wireless traffic.                                            |
| 1269523 | Rebooting the secondary FortiGate in HA active-passive mode causes traffic loss due to split-brain and unintended ARP broadcasts from the secondary FortiGate. |
| 1271901 | Authentication issues occur when Azure SDN connectors reuse incorrect tenant tokens after HA failover                                                          |
| 1273912 | Split-Brain state occurs when configuring a new VDOM when the primary has more VDOM license seats than the secondary unit                                      |
| 1275737 | License Status: Warning occurs when root VDOM is active on the primary in a FortiGate-VM HA A/P cluster with VDOMs and virtual clustering enabled.             |
| 1281897 | Missing start time occurs when running diagnose sys ha dump-by group after upgrading to 7.6.6                                                                  |
| 1286934 | Authentication issues occur in FortiCloud SSO during HA failover due to serial mismatch                                                                        |
| 1292490 | HA settings are lost when upgrading from 7.4.11 to 7.6.6 with an HA heartbeat interface configured with VRF 1                                                  |

## HyperScale

| Bug ID  | Description                                                                        |
|---------|------------------------------------------------------------------------------------|
| 1219541 | Traffic disruption occurs when changing an interface's vdom                        |
| 1220140 | FGT doesn't support user logging with /64 framed-IPv6-Prefix in radius accounting. |
| 1223847 | Excessive hyperscale logs occur when log-mode is set to per-mapping                |

| Bug ID  | Description                                                                 |
|---------|-----------------------------------------------------------------------------|
| 1245165 | ICMPv6 type 2 packets are dropped when SIP ALG and Hyperscale are activated |
| 1284721 | BFD sessions drop when running diagnose firewall ippool list pba            |
| 1291520 | DNS traffic drops occur when BGP to router 2 goes down                      |

## IPsec VPN

| Bug ID  | Description                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------------------|
| 1127782 | Traffic is dropped by anti-spoof check when passing traffic through phase2 transport mode with GRE encap.                 |
| 1157829 | Timeout occurs when incorrect timeout is used for 2FA with FortiClient and RADIUS server authentication                   |
| 1176036 | DHGRP mismatch occurs when FortiGate pushes VPN config to FortiExtender for lan-extension                                 |
| 1200084 | IPsec tunnel dec/enc counters fail to update when NPU offloading is enabled                                               |
| 1201212 | Reply traffic is dropped when anti-spoof check fails                                                                      |
| 1209759 | IKEv2 connection fails with "gw validation failed" error when the peer's ASN1DN ID contains multiple OU fields            |
| 1211532 | Traffic drop occurs when anti-spoof check fails due to mismatched source IP and selector range in IPsec VPN               |
| 1213238 | Authentication issues occur when syncing Fortiidentity Cloud users through LDAP for IPsec IKEv2 tunnel with EAP-TTLS      |
| 1215724 | IPsec tunnel establishment fails when FIPS-CC mode is enabled and DH group 31 or 32 is used.                              |
| 1217216 | DHCP requests fail when FortiGate sends the full DN instead of the CN in Option 61 during IKEv2                           |
| 1217988 | ADVPN Dynamic BGP remains active after IPSEC disconnection when Bring Down -> Entire Tunnel is used on the parent tunnel. |
| 1218530 | Error condition occurs when using Duo Proxy LDAP application with MFA                                                     |
| 1220562 | Traffic is offloaded when IPsec tunnel is configured with interface set to VNE tunnel interface                           |
| 1227222 | IKEv1 transport mode issue occurs when FortiGate is behind a NAT device                                                   |
| 1229448 | IKEv2 peer selection fails when using AES256GCM-PRFSHAxxx encryption proposal.                                            |
| 1238778 | Decrypt counters fail to update when NPU offload is enabled                                                               |
| 1245740 | MTU reduction occurs when using IPsec with GCM on 9xG and 12xG devices                                                    |

| Bug ID  | Description                                                                                                                          |
|---------|--------------------------------------------------------------------------------------------------------------------------------------|
| 1246635 | IPsec tunnel disruption occurs when Phase-2 rekey completes with incorrect CHILD-SA deletion.                                        |
| 1248524 | File download fails when FortiGate encounters IPSec VPN with set encapsulation vpn-id-ipip and AV proxy and NAT-T                    |
| 1249753 | Old assigned IP address remains in routing table when tunnel is flushed or renegotiated on client side with mode-cfg enabled.        |
| 1252546 | Negotiation timeout occurs when entering OTP within 120 seconds validity period                                                      |
| 1257646 | High CPU usage occurs when using IPsec over TCP and receiving an RST packet                                                          |
| 1263848 | IKEv2 CERTREQ matching failure occurs when FortiGate acts as a common VPN server for multiple vendors with multiple CA certificates. |
| 1264833 | SAML IPSEC VPN connection fails when connected to a WiFi network via Tunnel SSID                                                     |
| 1278723 | Traffic forwarding issues occur when MTU constraints are not properly configured for IPsec tunnels                                   |
| 1278940 | Unexpected behavior occurs in the system when receiving IPsec VPN traffic with large ICMP packets and NPU offload enabled            |
| 1287274 | Loopback-asymroute option is not configurable when transport is set to auto.                                                         |

## Intrusion Prevention

| Bug ID  | Description                                                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1040242 | When Inline IPS is enable and the videofilter profile has both channel and cateogry, youtube channel main page will not be blocked.                           |
| 1156490 | When inspection mode is proxy, inspect-all is enabled and http-policy-redirect is enabled, traffic is not sent to WAD for processing and consequently dropped |
| 1168037 | Error condition occurs in proxy mode when using inspect-all certificate-inspection in ssl-ssh-profile                                                         |
| 1208885 | DSCP 7 marking is not applied when Windows Update traffic is not application-identified in a VDOM.                                                            |
| 1244350 | MCDB update issues occur when FortiGate is configured with NGFW policy mode                                                                                   |
| 1268468 | UDP fragmentation bypasses IPS when NP is enabled in IPsec tunnel                                                                                             |
| 1273729 | Error condition in IPS occurs when handling high volumes of application traffic through FortiGate                                                             |

## Log and Report

| Bug ID  | Description                                                                                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1116246 | An error condition in locallogd occurs when the system enters memory conserve mode                                                                                                  |
| 1185876 | Log daemon resolves server IP reliably when using dnsproxy daemon                                                                                                                   |
| 1198455 | When running ITS test occasionally the wrong link status reading is logged                                                                                                          |
| 1223900 | Execution log failure occurs when sending test-connectivity from SSH                                                                                                                |
| 1225145 | Error condition in miglogd occurs when the system is under heavy pressure or in memory conserve mode.                                                                               |
| 1226196 | HTTP transaction log displays IP instead of URL when client disconnects before server response forwarding                                                                           |
| 1229712 | Failed to get FAZ's status occurs when changing static route settings                                                                                                               |
| 1236184 | An error condition in locallogd occurs when disk space is full on FortiGate.                                                                                                        |
| 1237774 | Log field information loss occurs when the URL or Referrer header exceeds a certain character limit                                                                                 |
| 1239708 | Logs are not written to the disk queue when the memory queue reaches its limit.                                                                                                     |
| 1240481 | IPS log-packet files are not cleaned up when retention time exceeds maximum-log-age                                                                                                 |
| 1241256 | Failure to send OT information to FortiAnalyzer occurs when a large number of IoT/OT vulnerabilities are generated.                                                                 |
| 1253334 | Intermittent disconnection of FortiAnalyzer from FortiGate caused by excessive TPM requests from httpsd.                                                                            |
| 1261240 | Repeated DNS resolution attempts occur when related functionality is disabled on FortiGate                                                                                          |
| 1265088 | Syslog packets are sent when syslog-override is enabled                                                                                                                             |
| 1266492 | Secondary unit logs are not received by FortiAnalyzer Cloud when running FortiOS 7.4.9 and above in a FortiGate HA cluster                                                          |
| 1269067 | Synchronization fails when generating a large number of IoT/OT vulnerabilities                                                                                                      |
| 1272019 | An error condition occurs in the GeoIP database during updates                                                                                                                      |
| 1281143 | IPS archive logging fails after firmware upgrade to v7.6.6 due to incorrect folder permissions. Affects only FortiGates which have been upgraded from a version earlier than 6.4.2. |

## Proxy

| Bug ID  | Description                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1171499 | Certificate chain is not sent during SSL inspection after upgrade.                                                                                                                      |
| 1189141 | An error condition in WAD occurs when handling large query responses.                                                                                                                   |
| 1190329 | Memory usage issues caused by insufficient resources during application processing                                                                                                      |
| 1213247 | 504 Gateway Timeout shown when a virtual-server configured in full mode connects to a HTTPS server that only supports TLS <= 1.2 and which also only supports using SHA1 for signatures |
| 1224915 | Intermittent page could not be reached issue occurs when authentication is required by QUIC                                                                                             |
| 1230674 | UTM profiles for SMTP(s)/POP3(s)/IMAP(s)/NNTP in proxy-mode policy on low-RAM models lack feature-set option.                                                                           |
| 1233324 | High memory usage occurs when inline IPS is enabled with long-lived connections and IPS DB updates.                                                                                     |
| 1247379 | CPU usage issues observed during large HTTPS downloads                                                                                                                                  |
| 1255610 | TLS active probe failure occurs when proxy inspection is enabled                                                                                                                        |
| 1281435 | SSL deep inspection is bypassed when Firewall Policy is configured with WAF and proxy-based inspection.                                                                                 |
| 1286767 | Certificate selection issue occurs when multiple certificates are defined in an SSL profile in replace mode                                                                             |

## Routing

| Bug ID  | Description                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------|
| 1151848 | IPv6 BGP flap occurs when FortiGate FGSP cluster connects to Dell Sonic                                |
| 1162962 | BGP service disruption occurs when the LAG interface flaps                                             |
| 1230742 | VXLAN connectivity issues occur when configured with inter-VDOM IPsec underlay between two FortiGates. |
| 1233456 | OSPF6 route database loses routes when HA monitored interface flaps.                                   |
| 1243609 | Route flapping occurs when external routes are redistributed into BGP                                  |
| 1244747 | Traffic disruption occurs when using iSCSI boot volume after a reboot                                  |
| 1246350 | Traffic does not honor vrf-select when using loopback interface IP as source-ip                        |

| Bug ID  | Description                                                                                       |
|---------|---------------------------------------------------------------------------------------------------|
| 1246749 | Traffic drop occurs when Verizon Dynamic Network Mobility Routing is configured with a GRE tunnel |
| 1247150 | BGP session ends when interface is down in non-zero VRF after hold down timer expires             |
| 1247172 | BGP sessions remain down when using VRF option due to invalid BGP Identifier                      |
| 1251244 | OSPFv6 neighborship failure occurs when FortiGate is upgraded to FortiOS 7.6.5                    |
| 1269208 | BGP routes disappear from the FIB when pre-encapsulation is enabled on VPN Phase1.                |
| 1272281 | VRRP failure occurs when using hardware-switch on FortiGate                                       |
| 1273467 | Return traffic is not forwarded out of port15 when receiving GRE traffic via port15.              |
| 1279315 | Error condition in BGP process occurs when FIM failover sequence happens                          |

## SD-WAN

| Bug ID  | Description                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------|
| 1051429 | Dynamic BGP session remains on initial shortcut even when out of SLA.                                                       |
| 1138635 | Speed-test failure occurs when using ECMP routing configuration from Hub to Spoke.                                          |
| 1176538 | Traffic between spokes occurs when shortcut is out of SLA or dead with load balancing enabled and fib-best-match tie-break. |
| 1179004 | Speed test failures occur when running multiple tests concurrently on BGP over loopback designs                             |
| 1199707 | SIP traffic issue occurs when TCP syn-ack packets use a different egress interface than the syn packets.                    |
| 1203173 | SD-WAN member fails to return to active state after PPPoE interface instability                                             |
| 1203917 | SD-WAN interface status becomes Unknown when Health Check SLA is good                                                       |
| 1205633 | BGP on loopback uses the unstable 4G link instead of the primary fibre tunnel when establishing its TCP session.            |
| 1234194 | Non-participant members appear in latency and packet loss columns when viewing the performance SLA page                     |
| 1239537 | Speedtest failure occurs when total latency exceeds 800ms between HUB and Spoke.                                            |
| 1252011 | WAN outage occurs when upgrading FortiGate from 7.6.1 to 7.6.3 or 7.6.5 with SD-WAN and IPsec over VNE WAN links            |
| 1254899 | Unhealthy out-of-SLA BGP community is sent unexpectedly after HA switchover when all members are in-sla                     |
| 1279456 | Link-Monitor instability occurs when a dead monitor uses the same ICMP ID as a working monitor.                             |

## Security Fabric

| Bug ID  | Description                                                                                      |
|---------|--------------------------------------------------------------------------------------------------|
| 1076439 | Security fabric Asset Identity Center shows "Failed to load user device store data"              |
| 1225433 | Automation Stitch variable truncation occurs when using json-c version 0.18 with webhook actions |
| 1228317 | Local-in policy creation issue occurs when Security fabric is enabled on non-NPU VDOM links      |
| 1239953 | Automation stitches fail to execute when FortiAnalyzer sends a security-event notification       |
| 1244300 | Automation cli-script action runs in memory when triggered by automation.                        |
| 1254426 | Email notification failure occurs when HA failover happens in downstream FortiGate               |
| 1267107 | Memory usage issues caused by Security Rating running full reports                               |
| 1275814 | Loss of connectivity occurs when AKS cluster provisioning state is not Succeeded                 |

## Switch Controller

| Bug ID  | Description                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------|
| 947247  | Wired clients are not displayed in physical topology when connected to FortiSwitch.                                   |
| 1183725 | Outage occurs when modifying LLDP profile on multiple ports including FortiLink trunk ports                           |
| 1195908 | Virtual VLAN switch forwarding issues occur when STP is enabled in HA setups with multiple members on FortiGate-600F. |
| 1216623 | High CPU usage occurs when Fortilink IoT triggers packet capture in switch                                            |
| 1220590 | Intermittent connectivity loss occurs in FortiSwitches when upgrading FortiGate to v7.6.4                             |
| 1221779 | Device data is missing when querying FortiGate API on FortiOS v7.4                                                    |
| 1227202 | FortiSwitch configuration is erased when switch-controller fails to add port1 during reboot                           |
| 1229555 | Incorrect VLAN assignment occurs when NAC policies use hostname filters with NetBIOS Name Service group names.        |
| 1232304 | FortiSwitches go offline when upgrading FortiGate from 7.2.10 to 7.4.x                                                |
| 1238312 | VLANs from other VDOMs are not added to the port when allowed-vlans-all is enabled.                                   |
| 1239300 | Incorrect port information is displayed when running diag switch-controller switch-info port-stats command            |
| 1239751 | FortiSwitches go offline when upgrading FortiGate from 7.2.10 to 7.4.x                                                |

| Bug ID  | Description                                                                                                                                |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1244391 | Empty PORTID occurs when FortiGate switch-controller is connected to FortiSwitch stacking setup                                            |
| 1249243 | Ports fail to work when configured with the same settings as other working ports after VLAN reconfiguration in a FortiGate HA A-P cluster. |
| 1269920 | Firmware download fails when one firewall attempts to download FortiSwitch firmware from FortiGuard                                        |
| 1269995 | An error condition in fltund occurs during upgrade to 7.6.6                                                                                |
| 1275793 | Authorization issues occur with FortiExtender on FortiGate 201G with version 7.6.6                                                         |
| 1290022 | Device information fails to load when FortiSwitch has a duplicate prefix name                                                              |

## System

| Bug ID  | Description                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------|
| 1083626 | FortiGate 90G/91G auto-negotiate support for shared SFP ports.                                                                   |
| 1107623 | A warning occurs during disk scan when executing a factory reset                                                                 |
| 1113064 | Memory usage issues caused by running simulator stress test on FortiGate                                                         |
| 1116876 | VDSL connection failure occurs when configured on FortiGate 50G-DSL                                                              |
| 1137047 | An error condition occurs when entering FIPS-CC mode                                                                             |
| 1144387 | FortiGate 50G DSL fails to acquire an IP address from a DSL modem                                                                |
| 1149006 | DHCP lease delivery issues occur when auto-discovery-receiver is enabled and IPsec tunnels are flapping                          |
| 1157402 | Modem disconnects occur when using Verizon SIM with a strong signal                                                              |
| 1165059 | Unexpected behavior in system occurs when executing factory reset on FortiGate-70F                                               |
| 1165706 | SSH and Web CLI sessions are disconnected when generating a TAC Report.                                                          |
| 1167271 | Link LEDs on FortiGate 401F are lit when no cables are attached.                                                                 |
| 1169167 | VDOM link interfaces are not visible when single-vdom-npuvlink is enabled on non-NP7 platforms                                   |
| 1170716 | Failed attachment to tower occurs when using custom APN with FortiGate 50G-5G modem                                              |
| 1170933 | MTU inconsistency occurs when creating a new LACP interface without a member interface and then adding a member interface later. |
| 1179827 | Hardware switch configuration limitations occur when adding Wan1 and Wan2 on FortiGate                                           |

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1183678 | QSFP-28-CWDM4 transceivers in ports 33 and 34 of FortiGate 2600F show as down after upgrading to 7.6.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1188182 | DHCP server failure to deliver IP addresses occurs when auto-discovery-receiver is enabled and IPsec tunnels are flapping.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1188905 | Unresponsiveness occurs when MTU calculation is incorrect in function np_fragment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 1190267 | An error condition in search_core_tag occurs when rebooting FortiGate-3960E with B3589                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1191833 | Inaccurate LAN and WAN speed values occur when running the hardware NIC-led test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 1192303 | <p>On FortiGates with NP7 processors, the following new option is available to enable or disable VLAN accounting:</p> <pre>config system npu      set vlan-accounting {disable   enable}  end</pre> <p>VLAN accounting is enabled by default.</p> <p>VLAN accounting on a busy FortiGate with a large number of VLANs can generate large numbers of VLAN lookup (SPV/TPV) messages. In some cases these messages can cause CG-FULL conditions or packet drops, especially on very busy systems.</p> <p>You can use the following command to reduce the number of VLAN accounting messages that are generated by</p> <p>increasing the VLAN accounting interval.</p> <pre>config system npu      set vlan-acct-interval &lt;milliseconds&gt;  end</pre> <p>The default VLAN accounting interval is 200 milliseconds. The range is 100 to 10000 milliseconds.</p> |

| Bug ID  | Description                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------|
| 1197529 | Unable to free memory local user authentication until fnbamd restarted                                                          |
| 1198350 | MTU inconsistency occurs when using redundant interface with Jumbo MTU                                                          |
| 1198772 | High CPU usage issues observed during GTP traffic handling on multiple slave FPMs                                               |
| 1200220 | Intermittent disconnection of FortiAnalyzer from FortiGate caused by excessive TPM requests from httpsd.                        |
| 1209720 | LAN 1, 2, 3, and A speed LED issues occur during NIC-led test step 3.                                                           |
| 1209793 | Interface configuration is lost when FortiManager managed FortiGate reboots after a power cycle or unexpected shutdown          |
| 1214384 | Unexpected behavior in FortiGate occurs when processing IPv6 traffic with invalid destination entries.                          |
| 1214950 | Batch mode configuration of system admin is allowed without specifying admin credentials                                        |
| 1215120 | BLE light blinks blue when FortiGate is set up with FortiZTP without CLI login                                                  |
| 1215780 | Connection failure occurs when using a custom APN                                                                               |
| 1216658 | Packet drop occurs when traffic is initiated from the Internet to devices connected to the EMAC VLAN interface                  |
| 1217130 | VDOM removal occurs from dia sys vd list output when rebooting FortiGate with dedicated-mgmt enabled                            |
| 1217722 | CPU usage issues observed when dedicated-management-cpu is enabled on np6 platform                                              |
| 1217924 | Packet size issues occur when 802.1AD interface is based on a LACP interface with MTU set to 9216.                              |
| 1220898 | FortiGate becomes unresponsive when adding more than three 802.1ad interfaces                                                   |
| 1221196 | Optical port speed issues occur when connecting to Ericsson or Nokia radio nodes on FortiGate 90G/91G.                          |
| 1221738 | Returning packet is not forwarded via the expected LACP interface when set algorithm L3                                         |
| 1221994 | CPU usage issues observed during TX direction port mirroring                                                                    |
| 1223295 | MTU override size inconsistency occurs when changing mtu on aggregate interface with emac-vlan                                  |
| 1228420 | PCI device check fails when BIOS version is 07000203                                                                            |
| 1228807 | Some secret keys are not updated after a config change even when Private-Data-Encryption is enabled                             |
| 1228992 | Memory usage issues caused by exceeding device memory quota                                                                     |
| 1229804 | Unexpected behavior occurs in the system when handling ICMPv6 host unreachable error messages after IPv6 neighbor entry expires |

| Bug ID  | Description                                                                                                                          |
|---------|--------------------------------------------------------------------------------------------------------------------------------------|
| 1231510 | IP address assignment issues occur on DSL interfaces configured with static IP after reboot or at irregular intervals                |
| 1232383 | Unexpected behavior in the kernel occurs when running stressful multicast traffic through VXLAN in switch interface                  |
| 1235359 | Slowness occurs when renaming address objects                                                                                        |
| 1238186 | Error condition occurs when BGP neighbors are configured and IPv6 DHCP Client is enabled on WAN interface                            |
| 1238339 | Dedicated host queues occur when critical traffic like BFD, BGP, LACP is processed                                                   |
| 1238520 | Registration bypass option is available during the 7-day setup period                                                                |
| 1239336 | Central management configuration issues occur when using FortiGate GUI for Forticare registration                                    |
| 1244037 | Limited speed options occur on 1G RJ45 ports of FortiGate 200F and 201F.                                                             |
| 1244259 | Console becomes unresponsive due to being overwhelmed by excessive logging when cpu stalls occur.                                    |
| 1246081 | Memory usage issues caused by running v4/v6 routing protocols                                                                        |
| 1246315 | An error condition in snmpd occurs when querying fgLicVersion                                                                        |
| 1246914 | Unexpected behavior in the kernel occurs when forwarding ICMP error messages from NAF devices                                        |
| 1248631 | Intermittent reboot issues occur in FortiWiFi-50G when WiFi clients connect via RADIUS or ax bands                                   |
| 1249410 | Incomplete data erasure occurs on FortiGate-60F when executing erase-disk SYSTEM command                                             |
| 1251011 | FOS signature verification failure occurs when burning image on FGT-30G and FGT-31G.                                                 |
| 1254396 | BLE LED continuously blinks Light Blue when using FortiZTP setup without CLI login                                                   |
| 1254702 | Unexpected behavior in the kernel occurs when handling IPv6 neighbor traffic within a subnet                                         |
| 1255091 | Bluetooth remains active when configured with FortiZTP without CLI login                                                             |
| 1255825 | Conserve mode may occur when running full Security Rating report devices that have hundreds of extension devices (such as FortiAPs). |
| 1255973 | CPU usage issues observed during GUI session queries                                                                                 |
| 1256212 | An error condition in cmdbsvr occurs when FIPS-CC mode is enabled on FortiGate-60F                                                   |
| 1257265 | An error condition in SNMP occurs when querying fgVWLHealthCheckLinkTable on FortiOS 7.6.4                                           |
| 1259458 | Intermittent reboot of FortiGate-71G caused by an error condition in the IPS engine.                                                 |

| Bug ID  | Description                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------|
| 1261088 | An error condition in the connection daemon occurs when configuring a broadcast IP address on a FortiGate interface via CLI |
| 1263001 | IPsec dial-up instability occurs over WWAN interface on FortiGate 51G after upgrading from 7.4.9 to 7.4.11                  |
| 1264495 | Throughput drops to 0 during netperf testing on FGT200G and FGT201G caused by 1G SFP autoneg enabled.                       |
| 1264805 | Unexpected behavior in the system occurs when upgrading to 7.4.9                                                            |
| 1265180 | Memory usage issues caused by logging on FortiCarrier-4400F                                                                 |
| 1266447 | Inconsistent values occur when querying SNMP OID 'fg5gMdmOpMode'                                                            |
| 1267113 | LLDP advertised Sysname truncation occurs when a local domain is configured                                                 |
| 1267635 | An error condition occurs in the system during disk scan execution                                                          |
| 1268947 | High CPU usage occurs when creating or editing a VLAN interface via the web UI                                              |
| 1271792 | Failover to secondary IP does not occur when primary Fgfm connection is down                                                |
| 1275296 | No reply occurs when EMAC-VLAN receives ICMP requests on FortiGate 601E                                                     |
| 1276029 | Creating a virtual wire pair on bypass models results in a memory leak                                                      |
| 1276129 | Unexpected behavior in WAD procmgr occurs when mounting chroot jails on FortiOS 7.6.6                                       |
| 1280597 | DHCP scope subnet mismatch occurs when default management IP is 192.168.2.99 after factory reset                            |

## Upgrade

| Bug ID  | Description                                                                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1135049 | After a FortiOS upgrade, an error condition occurs when update daemon tries to update the databases while CMDB is still loading the JSON file at the same time. |
| 1155333 | FGT/FWF-3XG upgrade fails with error "inflate failed: round 1, err -3" when memory usage is high                                                                |
| 1193036 | Inconsistency occurs when auto-firmware-upgrade-start-hour default value is checked                                                                             |
| 1243233 | Configuration load failure occurs when upgrading to 7.6.5 through FortiManager                                                                                  |
| 1250292 | From a FGT-121G, upgrading a fabric device FSW-T1024E fails                                                                                                     |
| 1252663 | On FortiGate D-series devices running older BIOS versions, the serial number changes to FGT0000000000001 after upgrading to FortiOS 7.4.10,7.4.11,7.6.5,7.6.6.  |

| Bug ID  | Description                                                                                           |
|---------|-------------------------------------------------------------------------------------------------------|
| 1256067 | Required automatic upgrade may not complete successfully when device is unlicensed or end-of-support. |
| 1283092 | Upgrade failure occurs when Private Data Encryption is enabled                                        |

## User and Authentication

| Bug ID  | Description                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------|
| 1148209 | Auto-enrolment for EC certificate using SCEP fails when reading inner PKCS#7                                               |
| 1169349 | Assignment of FortiToken through FortiManager fails when FortiGate is configured.                                          |
| 1177519 | Login failure occurs when attempting to access admin user without a username query parameter                               |
| 1204356 | Fortinet_CA2 is missing when loaded with new CA2 supported BIOS                                                            |
| 1211983 | Certificate chain issues occur when firewall encounters a certificate renewal issue while using EST simplereenroll process |
| 1212700 | Authentication failure occurs when system zone name conflicts with VDOM name                                               |
| 1214438 | Failover to secondary Tacacs+ server occurs when primary server is unreachable.                                            |
| 1215197 | An error condition in fnbamd occurs when downloading intermediate CAs through multiple AIA links                           |
| 1217617 | Login failure occurs when a trusted host is set for the admin after upgrading FortiGate to version 7.4.9                   |
| 1218458 | Hardware token activation fails when CMDB write permission is enforced.                                                    |
| 1227685 | An error condition in fnbamd occurs when FortiGate attempts to download intermediate CAs through multiple AIA links        |
| 1228793 | Certificate auto-enrollment via CMPv2 fails when using an intermediate CA cert after upgrading                             |
| 1233862 | Certificate renewal through EST protocol fails when DNS lookup fails                                                       |
| 1236839 | An error condition in fnbamd occurs when referencing two peer users during certificate authentication                      |
| 1237504 | An error condition in fnbamd occurs when processing DNS responses with multiple IP addresses                               |
| 1239951 | Hardtoken activation fails when CMDB write permission is enforced                                                          |
| 1243758 | SCEP enrollment fails when sending GetCACaps request without CA name mark due to server error                              |
| 1244268 | Fnbamd error when downloading intermediate CAs through multiple AIA links                                                  |

| Bug ID  | Description                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 1246613 | Radius CoA disconnection fails when sending a CoA Disconnect Request with a Calling-Station-Id on FortiOS 7.6                               |
| 1247109 | Authentication issues occur when editing a vdom CA certificate with VDOM enabled                                                            |
| 1251941 | An error condition occurs in EAB when entering an HMAC value with a 66-byte key.                                                            |
| 1252114 | Tokens cannot be found when using a drift screen size of 1                                                                                  |
| 1253914 | TACACS+ accounting logs are not generated when setting up a connection to the Tacacs+Accounting server with per VDOM interfaces configured. |
| 1259154 | Authentication failure occurs when certificate rotation happens on Standalone HA primary FortiGate                                          |
| 1263865 | Connection failure occurs when maximum session limit is reached with EAP enabled in IKE config and TFA for users.                           |
| 1266066 | Authentication failure occurs when using FortiToken for two-factor authentication after upgrading from FortiOS 7.6.4 to 7.6.5               |

## VM

| Bug ID  | Description                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------|
| 1041341 | Error condition occurs when using vlink0 with HTTPS on FGT-VM-AZURE                                                      |
| 1102434 | Configuring VRF on hbdev will cause FortiGate VM HA not Syncing                                                          |
| 1217942 | FQDN synchronization issues occur when the primary's timeout value on the secondary is not refreshed in a timely manner. |
| 1218373 | Auto-scale failure occurs when creating FGT-AWS auto scale group with AWS CloudFormation                                 |
| 1223933 | Loss of VWP configuration occurs when rebooting with unreferenced member interfaces                                      |
| 1228324 | Azure SDN connector fails to update new subscriptions until restarted.                                                   |
| 1239551 | Image publishing issue occurs when signing shim bootloader with Fortinet CA on Azure                                     |
| 1245936 | FGT-VM failed to validate vm license from FortiManager with ipv6 address                                                 |
| 1260183 | License validation occurs when FortiGate is connected to FortiManager in an air-gapped AWS environment                   |
| 1261051 | Boot failure occurs when Trusted Launch is enabled                                                                       |
| 1269889 | Dynamic objects are removed when FortiGate encounters a 503 Service Unavailable from Google Cloud Platform.              |
| 1272991 | Boot up failure occurs when confidential VM is enabled                                                                   |

| Bug ID  | Description                                                                                                       |
|---------|-------------------------------------------------------------------------------------------------------------------|
| 1274229 | Unexpected behavior occurs when sending UDP packets with a total frame length of 1536 bytes.                      |
| 1274753 | License status warning occurs when secondary FortiGate validates VM License after upgrading to v7.4.11 or v7.4.10 |
| 1278705 | Firewall policy sync fails when system auto-scale is enabled on AWS instance type c5n.xlarge                      |

## VoIP

| Bug ID  | Description                                                                         |
|---------|-------------------------------------------------------------------------------------|
| 1227757 | Unexpected RTP stream closure occurs when provisional-invite-expiry-time is reached |

## Wan Optimization

| Bug ID  | Description                                                                                                                          |
|---------|--------------------------------------------------------------------------------------------------------------------------------------|
| 1252420 | An error condition in WAD occurs when ignore-pnc is enabled for webcache and a HTTPS request is sent with a Pragma: no-cache header. |

## Web Filter

| Bug ID  | Description                                                                                    |
|---------|------------------------------------------------------------------------------------------------|
| 1166666 | Domain fronting block occurs when sending traffic with upper case domain name over HTTP 1.1    |
| 1227049 | YouTube channel main page cannot be blocked by channel filter when proxy-inline-ips is enabled |
| 1230414 | Improvements to resolve memory usage issues when logical-sn is enabled                         |
| 1232698 | Antiphish fails to block usernames with '.' character when enabled.                            |
| 1254458 | Authentication page is not displayed when webfilter category is set to authentication action   |
| 1261505 | Video Filter fails to effectively block videos after YouTube updated its API.                  |
| 1268027 | Video blocking issues occur when accessing YouTube from the main page with channel filters     |

## WiFi Controller

| Bug ID  | Description                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1105433 | Running 'diag wireless wlaac show all' during debugging causes unexpected AP disconnections in large-scale FAP deployments.                                                 |
| 1112629 | FAP offline and online again 30 seconds later after FortiGate HA failover                                                                                                   |
| 1158619 | 6GHz channels 1 to 93 are not available when AP-Country is set to Hungary                                                                                                   |
| 1192905 | Wireless-controller using direct RADIUS does not honour vrf-select and source-ip settings, resulting in incorrect VRF handling during authentication.                       |
| 1213368 | AP information is missing from forward traffic logs (of captive-portal SSID)                                                                                                |
| 1217779 | An error condition in cw_acd occurs when dedicated-mgmt is enabled                                                                                                          |
| 1218025 | Radius COA functionality does not work as intended when using an FQDN radius server with WiFi 802.1x authentication.                                                        |
| 1219415 | Connection failures may occur when WiFi clients authenticate using 802.1X and multiple IP addresses are resolved for the RADIUS server FQDN.                                |
| 1221283 | Clients unexpectedly keep moving between FAPs after frequency handoff from 5G to 2.4G due to obsolete BTSM request                                                          |
| 1227978 | Wi-Fi clients cannot maintain previous IP addresses after roaming from one FAP to another in the inter-controller layer-3 roaming topology.                                 |
| 1230455 | SSID loss occurs on FortiGate models when DARRP channel optimization fails.                                                                                                 |
| 1232763 | WiFi clients experience initial connectivity and packet-loss during roaming only on WPA2-Enterprise SSID with External RADIUS                                               |
| 1240269 | The virtual MAC address of Tunnel VAP interfaces changes unexpectedly after FortiGate HA failover or reboot when adding a wireless-controller.vap with quarantine disabled. |
| 1243404 | Roaming fails when 802.11r is enabled on WPA2-Enterprise with invalid PMKID                                                                                                 |
| 1243456 | FT reassociation fails when 802.11r is enabled on WPA2-Enterprise                                                                                                           |
| 1254074 | Duplicate Reassociation Responses were sent to same Wi-Fi client roaming between two FortiAP units                                                                          |
| 1256821 | The class attribute fails to restore when a Wi-Fi client roams between FortiGate access points using 802.11r.                                                               |
| 1257588 | WiFi clients experience random disconnections on WPA3-Enterprise SSID with External RADIUS                                                                                  |

## ZTNA

| Bug ID  | Description                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------------------|
| 987129  | Access denied occurs when favicon.ico is sent by browser during ZTNA SSH session with SAML auth                               |
| 1229620 | Redirect failures occur when VIP ports do not match real server ports                                                         |
| 1240300 | An error condition in WAD occurs when using ZTNA Web Portal and SSH bookmarks with specific authentication settings.          |
| 1253873 | SNAT failure occurs when ZTNA access-proxy policy uses IP pool                                                                |
| 1254981 | Error condition in WAD occurs when ZTNA proxy with SAML authentication for RDP is used without daily restarts.                |
| 1257675 | Connection error when didn't set sso and didn't set username and password for VNC bookmark when connecting to UltraVNC server |
| 1272422 | File uploads to SMB servers are not working in the ZTNA Web Portal because of a javascript error                              |
| 1278235 | Incorrect keyboard layout occurs when using ZTNA web portal                                                                   |

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 67](#)
- [Existing known issues on page 67](#)

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

## New known issues

Currently no new issues have been reported in 7.6.7.

## HyperScale

| Bug ID  | Description                                                                                    |
|---------|------------------------------------------------------------------------------------------------|
| 1245870 | An error condition in NPD occurs when setting SD-WAN interface member under full-offload level |
| 1285581 | Performance drop occurs when running TCP CPS PBA log and NAT with overload on FortiGate 4401F  |
| 1295024 | FGT 4201F B3688 has increase in performance by ~100% for CPS PBA eimoff eifoff log2host        |

## System

| Bug ID  | Description                                                                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1271259 | Transceiver issue occurs when using FR-1 QSFP 100G with FortiGate<br><b>Workaround:</b> Set mediatype to LR4 and disable forward-error-correction when speed is 100Gfull |

## Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.7.

## Agentless VPN

| Bug ID  | Description                                                   |
|---------|---------------------------------------------------------------|
| 1173772 | Unable to connect to SMB over SSLVPN web mode in FIPS-CC mode |

## Endpoint Control

| Bug ID  | Description                                                                            |
|---------|----------------------------------------------------------------------------------------|
| 1019658 | On FortiGate, not all registered endpoint EMS tags are displayed in the GUI.           |
| 1038004 | FortiGate may not display the correct user information for some FortiClient instances. |

## Firewall

| Bug ID | Description                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|
| 959065 | On the Policy & Objects > Traffic Shaping page, when deleting or creating a shaper, the counters for the other shapers are cleared. |
| 990528 | When searching for an IP address on the Firewall Policy page, the search/filter functionality does not return the expected results. |

## FortiGate 6000/7000 Platform

| Bug ID  | Description                                                                                                                              |
|---------|------------------------------------------------------------------------------------------------------------------------------------------|
| 653335  | SSLVPN user status does not display on the FortiManager GUI.                                                                             |
| 835847  | password policy was not correctly updated when using automation stitch                                                                   |
| 936320  | When there is a heavy traffic load, there are no results displayed on any FortiView pages in the GUI.                                    |
| 950983  | Feature Visibility options are visible in the GUI on a mgmt-vdom.                                                                        |
| 994241  | On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7. |
| 1006759 | After an HA failover, there is no IPsec route in the kernel.<br><b>Workaround:</b> Bring down and bring up the tunnel                    |
| 1102072 | On the FortiGate 7000 platform, cmdbsvr CPU usage can be higher than normal for extended periods on one or more FPM.                     |

| Bug ID  | Description                                                                                                                                                                                                                                    |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1112582 | Under some conditions, such as during conserve mode, you may not be able to log into the FortiGate 6000 management board GUI or CLI or when you log into the management board console a message similar to fork failed() continuously repeats. |
| 1130491 | Traffic disruption occurs when WCCP is enabled on FortiGate<br><b>Workaround:</b> Direct all related traffic to master FPC                                                                                                                     |
| 1132294 | 7KF/v7.6.3/b3490: ip nat port-preserve feature is not working when client's source port doesn't fall under FPM's nat port-range                                                                                                                |
| 1162187 | 7KF/b3617, FortiAP retains the same image after the upgrade                                                                                                                                                                                    |
| 1171183 | 7KF-1/B3563: The Global Traffic widget do not loading after factory reset due to legacy auth disabled by default.                                                                                                                              |
| 1185869 | 7000F image build3583 (v7.6.4) Multicast traffic testing was not working.                                                                                                                                                                      |

## FortiView

| Bug ID  | Description                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------|
| 1034148 | The Application Bandwidth widget on the Dashboard > Status page does not display some external applications bandwidth data. |

## GUI

| Bug ID  | Description                                                                           |
|---------|---------------------------------------------------------------------------------------|
| 1223774 | Firewall policy GUI page shows 'no-inspection' for SSL when profile group is applied. |
| 1237136 | Dynamic VLANs are not visible on the GUI when a port-security-policy is applied       |

## HA

| Bug ID  | Description                                                                                                                                             |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1135376 | When HA members are not registered under the same FortiCare account, the HA cluster cannot obtain contract info of all members from FortiGuard servers. |

## HyperScale

| Bug ID  | Description                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------|
| 1030907 | With a FGSP and FGCP setup, sessions do not show on the HA secondary when the FGSP peer is in HA.                          |
| 1042011 | Observed 'NPD-0 :DEL PRP FAIL! 0xffffffff; NPD-0 :PRP ADD FAIL! 0xffffffff nat_type=00000044 block_sz=128 port_base=11000' |
| 1130107 | 4401f:Session-helper dns session is created by hw and can be seen in log2host table                                        |
| 1151441 | 4801F-HA) "ha1/ha2" port as hw-session-sync-dev shows out-of-sync even though it is connected to NP7                       |
| 1262881 | Hw session sync dev goes out of sync due to the discrepancy in lag driver between primary and secondary                    |

## IPsec VPN

| Bug ID  | Description                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1131269 | UESP packet drop occurs when VPN peer uses different source ports for IKE-NATT and UESP<br><b>Workaround:</b> Add a flow rule to work around the issue |

## Intrusion Prevention

| Bug ID  | Description                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1076213 | FortiGate with 4G memory might enter conserve mode during FortiGuard update when IPS or APP control is enabled.<br><b>Workaround:</b> Disable option 'proxy-inline-ips' under 'config ips settings'. |
| 1093769 | Unexpected IPS UTM logs may be generated in NGFW policy mode for unknown applications.                                                                                                               |

## Proxy

| Bug ID  | Description                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1035490 | The firewall policy works with proxy-based inspection mode on FortiGate models with 2GB RAM after an upgrade.<br><b>Workaround:</b> After an upgrade, reboot the FortiGate. |

## REST API

| Bug ID | Description                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------|
| 993345 | The router API does not include all ECMP routes for SD-WAN included in the get router info routing-table command. |

## Security Fabric

| Bug ID  | Description                                                                      |
|---------|----------------------------------------------------------------------------------|
| 1040058 | The Security Rating topology and results does not display non-FortiGate devices. |

## Switch Controller

| Bug ID  | Description                                                                                                                                                                                                                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1113304 | FortiSwitch are offline after FortiGate upgraded from v7.4.6 or v7.6.0 to v7.6.1 or later when LLDP configuration set to vdom/disable under FortiLink interface.<br><b>Workaround:</b> Add LLDP configuration lldp-reception, lldp-transmission to enable under FortiLink interface, or rebuild FortiLink interface. |

## System

| Bug ID  | Description                                                                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1041726 | Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.                                                                                                            |
| 1142465 | ARP entries age out quickly after a system reboot, despite a long reachable-time setting                                                                                                    |
| 1179259 | TCP traffic is impacted over VXLAN when auto-asic-offload and UTM both enabled under the policy.<br><b>Workaround:</b> Disable auto-asic-offload on the impacted policy                     |
| 1193085 | Proxy-arp configuration failure occurs when the proxy-arp address group exceeds 256 entries<br><b>Workaround:</b> Divide the subnet into multiple proxy-arp entries less than 256           |
| 1227167 | Memory usage issues caused by the node process<br><b>Workaround:</b> Enable web-svc-auto-restart by running the command:<br><br>config system global<br><br>set web-svc-auto-restart enable |

| Bug ID | Description |
|--------|-------------|
|        | end         |

## User and Authentication

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1082800 | When performing LDAP user search from the GUI against a LDAP server with large number of users (more than 100K), the FortiGate may experience slowness and freeze due to HTTPSD process consumes too much memory. User may need to kill the HTTPSD process or perform a reboot to recover.<br><b>Workaround:</b> User can perform LDAP user search via the CLI. |
| 1157003 | Agentless FSSO connector issues occur when using Windows 2025 due to MS introduced additional restrictions to remote Event log reading.                                                                                                                                                                                                                         |

## VM

| Bug ID  | Description                                                                           |
|---------|---------------------------------------------------------------------------------------|
| 1125805 | Unable to access the FortiGate VM web interface deployed on AWS when ACME is enabled. |

## Web Filter

| Bug ID  | Description                                                             |
|---------|-------------------------------------------------------------------------|
| 1040147 | Options set in ftgd-wf cannot be undone for a web filter configuration. |

# Built-in AV Engine

AV Engine 7.00054 is released as the built-in AV Engine.

# Built-in IPS Engine

IPS Engine 7.01187 is released as the built-in IPS Engine. Refer to the [IPS Engine Release Notes](#) for information.

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

## Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.



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

Copyright© 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.