



# Release Notes

FortiOS 7.6.2



**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 16, 2025

FortiOS 7.6.2 Release Notes

01-762-1114584-20250616

# TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>Change Log</b>   | <b>5</b>  |
| <b>Introduction and supported models</b>  | <b>6</b>  |
| Supported models  | 6         |
| FortiGate 6000 and 7000 support   | 6         |
| <b>Special notices</b>  | <b>7</b>  |
| FortiManager support for updated FortiOS private data encryption key                            | 7         |
| Hyperscale incompatibilities and limitations  | 8         |
| FortiGate 6000 and 7000 incompatibilities and limitations                                       | 8         |
| SSL VPN removed from 2GB RAM models for tunnel and web mode                                     | 9         |
| 2 GB RAM FortiGate models no longer support FortiOS proxy-related features                      | 9         |
| FortiGate VM memory and upgrade   | 10        |
| Hyperscale NP7 hardware limitation  | 10        |
| FortiGate cannot restore configuration file after private-data-encryption is re-enabled         | 10        |
| SSL VPN not supported on FortiGate 90G series models  | 11        |
| <b>RADIUS vulnerability</b>   | <b>12</b> |
| <b>2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology</b> | <b>13</b> |
| <b>Changes in default behavior</b>  | <b>14</b> |
| <b>Upgrade information</b>  | <b>15</b> |
| Fortinet Security Fabric upgrade  | 15        |
| Downgrading to previous firmware versions   | 17        |
| Firmware image checksums  | 17        |
| FortiGate 6000 and 7000 upgrade information   | 17        |
| Default setting of cp-accel-mode is changed to none on 2GB memory models                        | 18        |
| Policies that use an interface show missing or empty values after an upgrade                    | 19        |
| Managed FortiSwitch do not permit empty passwords for administrator accounts                    | 19        |
| SLBC FG-5001E primary blade fails to install image  | 20        |
| <b>Removed speed setting affects SFP+ interfaces after upgrade</b>                              | <b>21</b> |
| <b>Product integration and support</b>  | <b>22</b> |
| Virtualization environments   | 23        |
| Language support  | 23        |
| SSL VPN support   | 24        |
| SSL VPN web mode  | 24        |
| FortiExtender modem firmware compatibility  | 24        |
| <b>Resolved issues</b>  | <b>27</b> |
| FortiGate 6000 and 7000 platforms   | 27        |
| GUI   | 27        |
| HA  | 27        |
| Intrusion Prevention  | 28        |
| IPsec VPN   | 28        |

|   |           |
|---|-----------|
| SSL VPN .....                           | 28        |
| System .....                            | 28        |
| User & Authentication .....             | 29        |
| VM .....                                | 29        |
| <b>Known issues .....</b>               | <b>30</b> |
| New known issues .....                  | 30        |
| FortiGate 6000 and 7000 platforms ..... | 30        |
| Hyperscale .....                        | 30        |
| Existing known issues .....             | 31        |
| Endpoint Control .....                  | 31        |
| Firewall .....                          | 31        |
| FortiGate 6000 and 7000 platforms ..... | 32        |
| FortiView .....                         | 32        |
| GUI .....                               | 32        |
| HA .....                                | 33        |
| Hyperscale .....                        | 33        |
| Intrusion Prevention .....              | 33        |
| IPsec VPN .....                         | 34        |
| Log & Report .....                      | 34        |
| Proxy .....                             | 34        |
| REST API .....                          | 35        |
| Security Fabric .....                   | 35        |
| Switch Controller .....                 | 35        |
| System .....                            | 35        |
| Upgrade .....                           | 36        |
| User & Authentication .....             | 37        |
| VM .....                                | 37        |
| Web Filter .....                        | 37        |
| WiFi Controller .....                   | 37        |
| <b>Built-in AV Engine .....</b>         | <b>38</b> |
| <b>Built-in IPS Engine .....</b>        | <b>39</b> |
| <b>Limitations .....</b>                | <b>40</b> |
| Citrix XenServer limitations .....      | 40        |
| Open source XenServer limitations ..... | 40        |

# Change Log

| Date       | Change Description  |
|------------|---|
| 2025-01-28 | Initial release.  |
| 2025-01-30 | Updated <a href="#">Policies</a> that use an interface show missing or empty values after an upgrade on <a href="#">page 19</a> and <a href="#">Managed FortiSwitch</a> do not permit empty passwords for administrator accounts on <a href="#">page 19</a> . |
| 2025-02-04 | Updated <a href="#">Resolved issues on page 27</a> and <a href="#">Known issues on page 30</a> .  |
| 2025-02-12 | Updated <a href="#">Known issues on page 30</a> .   |
| 2025-02-27 | Updated <a href="#">Known issues on page 30</a> .   |
| 2025-03-03 | Updated <a href="#">Known issues on page 30</a> .   |
| 2025-03-10 | Updated <a href="#">Known issues on page 30</a> .   |
| 2025-03-17 | Updated <a href="#">Known issues on page 30</a> .   |
| 2025-03-31 | Updated <a href="#">Known issues on page 30</a> .   |
| 2025-04-14 | Added <a href="#">2 GB RAM FortiGate models</a> no longer support <a href="#">Security Rating and Security Fabric topology on page 13</a> .<br>Updated <a href="#">Resolved issues on page 27</a> and <a href="#">Known issues on page 30</a> .               |
| 2025-04-28 | Updated <a href="#">Resolved issues on page 27</a> and <a href="#">Known issues on page 30</a> .  |
| 2025-05-13 | Updated <a href="#">Resolved issues on page 27</a> .  |
| 2025-05-27 | Updated <a href="#">Resolved issues on page 27</a> .  |
| 2025-06-05 | Updated <a href="#">Changes in default behavior on page 14</a> .  |
| 2025-06-09 | Added <a href="#">Removed speed setting affects SFP+ interfaces after upgrade on page 21</a> .<br>Updated <a href="#">Known issues on page 30</a> .   |
| 2025-06-12 | Updated <a href="#">Known issues on page 30</a> .   |
| 2025-06-16 | Updated <a href="#">SSL VPN not supported on FortiGate 90G series models on page 11</a> .   |

# Introduction and supported models

This guide provides release information for FortiOS 7.6.2 build 3462.

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

## Supported models

FortiOS 7.6.2 supports the following models.

|                         |   |
|-------------------------|---|
| <b>FortiGate</b>        | FG-40F, FG-40F-3G4G, FG-60F, FG-61F, FG-70F, FG-71F, 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-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F |
| <b>FortiWiFi</b>        | FWF-40F, FWF-40F-3G4G, FWF-60F, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE  |
| <b>FortiGate Rugged</b> | FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G  |
| <b>FortiFirewall</b>    | FFW-1801F, FFW-2600F, FFW-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 7.6.2 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

- [FortiManager support for updated FortiOS private data encryption key on page 7](#)
- [FortiGate cannot restore configuration file after private-data-encryption is re-enabled on page 10](#)
- [Hyperscale incompatibilities and limitations on page 8](#)
- [FortiGate 6000 and 7000 incompatibilities and limitations on page 8](#)
- [SSL VPN removed from 2GB RAM models for tunnel and web mode on page 9](#)
- [2 GB RAM FortiGate models no longer support FortiOS proxy-related features on page 9](#)
- [FortiGate VM memory and upgrade on page 10](#)
- [Hyperscale NP7 hardware limitation on page 10](#)
- [SSL VPN not supported on FortiGate 90G series models on page 11](#)
- [RADIUS vulnerability on page 12](#)
- [2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology on page 13](#)

## 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.

### 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

Support for the FortiGate private-data-encryption key by the Device Manager in FortiManager 7.6.2 and earlier is unchanged. It automatically detects the remote FortiGate private-data-encryption key status and prompts the administrator to manually type the private key (see picture below). FortiManager 7.6.2 and earlier does not support the updated, random private-data-encryption key as the administrator will have no knowledge of the key generated in the FortiOS CLI command above. It will be supported in a later version of FortiManager.

#### Warning

The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

| Search... |                  |               |                |                           |
|-----------|------------------|---------------|----------------|---------------------------|
| Status    | Device Name      | IP Address    | Platform       | Private Data Encryption K |
| ?         | FGVM02TM24009410 | 172.18.36.216 | FortiGate-VM64 |                           |
|           |                  |               |                | 1                         |

Verify

Close

### FortiOS upgrade behavior

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 7.6.2 features.

## FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.6.2 features.



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

## SSL VPN removed from 2GB RAM models for tunnel and web mode

On FortiGate models with 2GB of RAM or below, the SSL VPN web and tunnel mode feature will no longer be 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-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)

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 have SSL VPN web and tunnel mode support.

---

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

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, starting from version 7.4.4, FortiOS no longer supports proxy-related features.

This change impacts the FortiGate 40F and 60F series devices, along with their variants. See [Proxy-related features no longer supported on FortiGate 2 GB RAM models](#) for more information.

## 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 setup VMs with at least 4 GB of RAM for optimal performance.

## 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 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
```

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

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

Consider migrating to using IPsec Dialup VPN for remote access. See [FortiOS 7.6 SSL VPN to IPsec VPN migration](#).

# 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

## 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 2GB RAM](#).

# Changes in default behavior

| Bug ID | Description  |
|--------|--|
| 949997 | LDAPS authentication behavior changed. FortiOS 7.6.1 and later enhances the security standards for LDAPS by requiring FortiOS to trust the server certificate during the TLS handshake. If the LDAP server's CA certificate was not present and is not added after upgrading to FortiOS 7.6.2, LDAPS authentication will fail. To ensure smooth operation, import the LDAP server's CA certificate to FortiGate prior to upgrading. For more details, see <a href="#">Configuring client certificate authentication on the LDAP server</a> . |

# 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 15</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 7.6.2 is verified to work with these Fortinet products. This includes:

|   |                              |
|---|------------------------------|
| <b>FortiAnalyzer</b>                          | • 7.6.2                      |
| <b>FortiManager</b>                           | • 7.6.2                      |
| <b>FortiExtender</b>                          | • 7.4.0 and later            |
| <b>FortiSwitch OS<br/>(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 or SSL VPN, FortiClient version 6.0 and later are supported.

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



When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.6.0, 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 7.6.2. When Security Fabric is enabled in FortiOS 7.6.2, all FortiGate devices must be running FortiOS 7.6.2.

---

## 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 7.6.2:

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 7.6.2 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.

After upgrading to version 7.4.6 or 7.6.1 GA or later, users must manually recreate these policies and assign them to the appropriate SD-WAN zone.

## 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.

---

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

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

# Removed speed setting affects SFP+ interfaces after upgrade

Starting in FortiOS 7.6.1, the `1000auto` speed setting is removed. If a FortiGate SFP+ port speed is set to `1000auto` before upgrade, the upgrade process automatically changes the setting to `1000full`. This change can cause the interface to go down when the connecting device has a different speed setting.

**Workaround:** After upgrade, align the port settings. Edit the port and set the speed to `1000full` to restore the connection.

```
config system interface
  edit <port>
    set speed 1000full
  next
end
```

# Product integration and support

The following table lists FortiOS 7.6.2 product integration and support information:

|                                       |   |
|---------------------------------------|---|
| <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 0319 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none"><li>• Windows Server 2022 Standard</li><li>• Windows Server 2022 Datacenter</li><li>• Windows Server 2019 Standard</li><li>• Windows Server 2019 Datacenter</li><li>• Windows Server 2019 Core</li><li>• Windows Server 2016 Datacenter</li><li>• Windows Server 2016 Standard</li><li>• Windows Server 2016 Core</li><li>• Windows Server 2012 Standard</li><li>• Windows Server 2012 R2 Standard</li><li>• Windows Server 2012 Core</li><li>• Novell eDirectory 8.8</li></ul></li></ul> |
| <b>AV Engine</b>                      | <ul style="list-style-type: none"><li>• 7.00034</li></ul>   |
| <b>IPS Engine</b>                     | <ul style="list-style-type: none"><li>• 7.01026</li></ul>   |

See also:

- [Virtualization environments on page 23](#)
- [Language support on page 23](#)
- [SSL VPN support on page 24](#)
- [FortiExtender modem firmware compatibility on page 24](#)

## 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, and 8.0.</li></ul>   |

## Language support

The following table lists language support information.

### Language support

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

## SSL VPN support

### SSL VPN web mode

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

#### Supported operating systems and web browsers

| Operating System                          | Web Browser   |
|---|---|
| Microsoft Windows 7 SP1 (32-bit & 64-bit) | Mozilla Firefox version 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             |



| FortiExtender model | Modem firmware image name    | Modem firmware file on Support site        | Geographical region |
|---------------------|------------------------------|--|---------------------|
| 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 7.6.2. To inquire about a particular bug, please contact [Customer Service & Support](#).

## FortiGate 6000 and 7000 platforms

| Bug ID  | Description   |
|---------|---|
| 1149405 | The image upgrade fails when performing a non-graceful update due to an ISIZE mismatch during verification. |

## GUI

| Bug ID  | Description  |
|---------|--|
| 1092489 | The config system fortiguard > fortiguard-anycast setting was changed to automatically disable when the FortiGuard page is shown on GUI. |
| 1110382 | Admin can log in to GUI (HTTPS) with password, even when <i>admin-https-pki-required</i> is enabled.                                     |

## HA

| Bug ID  | Description   |
|---------|---|
| 1108895 | In an FGSP cluster, enabling and disabling standalone-config-sync results in the local dev_base being deleted and synchronized with the peer, which leads to the absence of the dev_base. |

## Intrusion Prevention

| Bug ID  | Description   |
|---------|---|
| 1107445 | Remove IPS diagnose command <code>diagnose ips cfgscript run</code> . |

## IPsec VPN

| Bug ID              | Description   |
|---------------------|---|
| 110359              | ADVPN IPsec traffic over shortcut drops when IPsec tunnel rekeys.   |
| 1012615             | IPsec VPN traffic is dropped after upgrading to version 7.4.3.  |
| 1073670             | Unexpected behavior observed in the IKED during HA split-brain events when IPsec tunnels are configured to use DHCP.                        |
| 1085628,<br>1102547 | IPsec IKEv2 with certificate-based authentication and eap-enabled tunnel comes up, even though a certificate validation failure is present. |
| 1103594             | ADVPN IPsec traffic over shortcuts drops during IPsec tunnel rekey.   |

## SSL VPN

| Bug ID  | Description   |
|---------|---|
| 1077157 | FortiGate sends out expired server certificate for a given SSL VPN realm, even when the certificate configured in <code>virtual-host-server-cert</code> has been updated. |
| 1101837 | Insufficient session expiration in SSL VPN using SAML authentication.   |

## System

| Bug ID  | Description   |
|---------|---|
| 1102416 | Cannot push config <code>sfp-dsl enable</code> and vectoring under interface. |

## User & Authentication

| Bug ID  | Description   |
|---------|---|
| 1075207 | Errors may occur in the FNBAMD due to the presence of two wildcard-enabled remote administrators in separate VDOMs. |

## VM

| Bug ID  | Description   |
|---------|---|
| 1012000 | When unicast HA setup has a large number of interfaces, FGT Hyper-V takes a long time to boot up. |

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 30](#)
- [Existing known issues on page 31](#)

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

## New known issues

The following issues have been identified in version 7.6.2.

### FortiGate 6000 and 7000 platforms

| Bug ID  | Description   |
|---------|---|
| 1102072 | On the FortiGate 7000 platform, cmdbsvr CPU usage can be higher than normal for extended periods on one or more FPM.  |
| 1112581 | On the FortiGate 7000F platform, after upgrading from FortiOS 7.4.7 to 7.6.2, cmdbsvr CPU usage can be at 99% on one or more FPMs for several minutes. During high CPU usage, FortiGuard packets cannot be synchronized to the affected FPM(s).   |
| 1112582 | Under some conditions, such as during conserve mode, you may be unable to log in to the FortiGate 6000 management board GUI or CLI, or when you log in to the management board console, a message similar to fork failed() continuously repeats.  |
| 1116862 | Graceful upgrade of a FortiGate 7000E chassis to FortiOS 7.6.2 may fail for some configurations.  |
| 1118004 | On a FortiGate 7000E FGCP cluster, after using the <i>execute ha disconnect</i> command to disconnect a chassis from the cluster, you can't use the special management ports to connect to the FIM in slot 2 or to any of the FPMs of either chassis. You can still connect to the FIM in slot 1. |

## Hyperscale

| Bug ID  | Description   |
|---------|---|
| 1108263 | HA configurations are lost if <i>hw-sess-sync-dev</i> is configured with more interfaces than expected. (The expectation is two times the number of NP7 chips.) |

## Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.2.

### 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 <i>Policy &amp; Objects &gt; Traffic Shaping</i> page, when deleting or creating a shaper, the counters for the other shapers are cleared.  |
| 990528  | When searching for an IP address on the <i>Firewall Policy</i> page, the search/filter functionality does not return the expected results.   |
| 994986  | The <i>By Sequence</i> view in the Firewall policy list may incorrectly show a duplicate implicit deny policy in the middle of the list. This is purely a GUI display issue and does not impact policy operation.<br>The <i>Interface Pair View</i> and <i>Sequence Grouping View</i> do not have this issue.  |
| 1117165 | Leaving the apn field empty in a GTP APN traffic shaping policy means that the policy will not match any traffic. Consequently, APN traffic shaping can only be applied to specific APNs.<br>To configure GTP APN traffic shaping:<br><pre>config gtp apn-shaper   edit &lt;policy-id&gt;     set apn [&lt;apn-name&gt; &lt;apngrp-name&gt; ...]     set rate-limit &lt;limit&gt;     set action {drop   reject}     set back-off-time &lt;time&gt;   next end</pre> |

## FortiGate 6000 and 7000 platforms

| Bug ID  | Description  |
|---------|--|
| 653335  | SSL VPN user status does not display on the FortiManager GUI.  |
| 790464  | After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.                              |
| 936320  | When there is a heavy traffic load, there are no results displayed on any <i>FortiView</i> pages in the GUI.                             |
| 950983  | <i>Feature Visibility</i> 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. |
| 998615  | When doing a GUI-packet capture on FortiGate, the through-traffic packets are not captured.  |
| 1006759 | After an HA failover, there is no IPsec route in the kernel.<br><b>Workaround:</b> Bring down and bring up the tunnel.                   |
| 1014826 | SLBC does not function as expected with IPsec over TCP enabled.  |

## FortiView

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

## GUI

| Bug ID  | Description   |
|---------|---|
| 853352  | When viewing entries in slide-out window of the <i>Policy &amp; Objects &gt; Internet Service Database</i> page, users cannot scroll down to the end if there are over 100000 entries.                              |
| 1047146 | After a firmware upgrade, a VLAN interface used in IPsec, SSL VPN, or SD-WAN is not displayed on the interface list or the SD-WAN page and cannot be configured in the GUI.   |
| 1047963 | High Node.js memory usage when building FortiManager in Report Runner fails. Occurs when FortiManager has a slow connection, is unreachable from the FortiGate (because FMG is behind NAT), or the IP is incorrect. |



## HA

| Bug ID  | Description  |
|---------|--|
| 851743  | When running the <code>diag sys ha checksum cluster</code> command, a previous line result is added further down in the output instead of new line result when a FortiGate is configured with several VDOMs. |
| 1137565 | vSN support added in 7.2.9, 7.4.6, and 7.6.1. FG-100F/101F do not yet support vSN and logical-sn.<br>No workaround until the devices support vSN.  |

## Hyperscale

| Bug ID  | Description   |
|---------|---|
| 1013892 | Unexpected behavior observed in NPD when the threat feed object attempted to update manually in the HA pair.  |
| 1042011 | On FortiGate, an login error message displays in the event log after completing an automation.  |
| 1089281 | For FG-480xF/FFW-480xF, using <code>npu-group</code> other than 0 with <code>log2host</code> around ~1M CPS could result in NP chip getting stuck.        |
| 1093287 | Using fixed-allocation IP Pools may cause NP7 NSS/PRP modules to become stuck, potentially disrupting traffic. Other PBA IP pools do not have this issue. |

## Intrusion Prevention

| Bug ID  | Description   |
|---------|---|
| 1076213 | FortiGate's with 4GB memory might enter conserve mode during the FortiGuard update when IPS or APP control is enabled.<br><b>Workaround:</b> Disable the <code>proxy-inline-ips</code> option under <code>config ips</code> settings.   |
| 1117043 | After upgrade, event log shows <code>logdesc="IPSA driver update failed" msg="Fail to update IPSA driver status!"</code> .<br>This issue only affects physical FortiGate models with the following IPS engine versions: <ul style="list-style-type: none"> <li>IPS Engine version: 7.550 - 7.567</li> <li>IPS Engine version: 7.1019 - 7.1039</li> </ul> To determine the IPS Engine versions, use the command: <pre>get sys fortiguard-service status   grep 'IPS/FlowAV Engine'</pre> <b>Workaround:</b> Power off the FortiGate. Wait 30 seconds, and then power on the FortiGate. |

| Bug ID | Description  |
|--------|--|
|        | <b>Note:</b> Reboot using the CLI is not an effective workaround and requires additional steps. After executing <code>exec shutdown</code> , unplug the power to the FortiGate. Wait one minute, and the power on the FortiGate. |

## IPsec VPN

| Bug ID  | Description  |
|---------|--|
| 735398  | On FortiGate, the IKE anti-replay does not log duplicate ESP packets when SA is offloaded in the event log.            |
| 995912  | After a firmware upgrade, some VPN tunnels experience intermittent signal disruptions causing traffic to be re-routed. |
| 1042371 | RADIUS authentication with EAP-TLS does not work as expected through IPsec tunnels.                                    |
| 1103754 | Failed HTTP sessions occur when passing through nTurbo due to improper handling of fragmented packets                  |

## Log & Report

| Bug ID | Description   |
|--------|---|
| 611460 | On FortiOS, the <i>Log &amp; Report &gt; Forward Traffic</i> page does not completely load the entire log when the log exceeds 200MB. |

## Proxy

| Bug ID  | Description   |
|---------|---|
| 1023054 | After an upgrade on a 2GB FortiGate device, the firewall policy does not switch from <i>Proxy-based</i> to <i>Flow-based</i> in the <i>Inspection mode</i> field.           |
| 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  |
|--------|--|
| 938349 | Unsuccessful API user login attempts do not get reset within the time specified in <code>admin-lockout-threshold</code> .      |
| 993345 | The router API does not include all ECMP routes for SD-WAN included in the <code>get router info routing-table</code> command. |

## Security Fabric

| Bug ID  | Description   |
|---------|---|
| 903922  | Physical and logical topology is slow to load when there are a lot of managed FortiAP devices (over 50). This issue does not impact FortiAP management and operation. |
| 1011833 | FortiGate experiences a CPU usage issue in the <code>Node.js</code> daemon when there multiple administrator sessions running simultaneously.                         |
| 1019844 | In an HA configuration, when the primary FortiGate unit fails over to a downstream unit, the previous primary unit displays as being permanently disconnected.        |
| 1040058 | The Security Rating topology and results does not display non-FortiGate devices.  |

## Switch Controller

| Bug ID  | Description  |
|---------|--|
| 961142  | An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.   |
| 1113304 | FortiSwitch units are offline after FortiGate is upgraded from 7.4.6 or 7.6.0 to 7.6.1 or later when LLDP configuration is set to <code>vdom/disable</code> under the FortiLink interface.<br><b>Workaround:</b> In LLDP configuration, enable <code>l1dp-reception</code> and <code>l1dp-transmission</code> under the FortiLink interface, or rebuild the FortiLink interface. |

## System

| Bug ID | Description  |
|--------|--|
| 947982 | On NP7 platforms, DSW packets are missing resulting in VOIP experiencing performance issues during peak times. |

| Bug ID  | Description  |
|---------|--|
| 971466  | FortiGateRugged 60 models may experience packet loss when directly connected to Cisco switch.  |
| 1041726 | Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.   |
| 1046484 | After shutting down FortiGate using the <code>execute shutdown</code> command, the system automatically boots up again.                                    |
| 1047085 | The FortiOS GUI is unresponsive due to a CPU usage issue with the <code>csfd</code> and <code>node</code> processes.                                       |
| 1058256 | On FortiGate, interfaces with DAC cables remain down after upgrading to version 7.4.4.   |
| 1069208 | If the DHCP offer contains padding when DHCP relay is used, the DHCP relay deletes the padding before relaying the packet.                                 |
| 1103146 | Duplicated RADIUS packets are captured by the sniffer when performing firewall authentication with a RADIUS server.  |
| 1103617 | Integrating an interface does not work when adding a new member into an existing interface or creating a new interface.                                    |
| 1112376 | Unexpected behavior observed in the <code>newcli</code> daemon due to inconsistencies in node registration between <code>cmdbsvr</code> and other daemons. |

## Upgrade

| Bug ID  | Description   |
|---------|---|
| 1043815 | Upgrading the firmware for a large number (100+) of FortiSwitch or FortiAP devices at the same time may cause performance issues with the GUI and some devices may not upgrade.<br><b>Workaround:</b> pace out the upgrade schedule and upgrade devices in smaller batches.   |
| 1097503 | Fabric upgrade from 7.2.9 to 7.4.5 failed.  |
| 1104649 | In 7.6.1 and 7.6.2, if a local-in policy, local-in-policy6, DoS policy, interface policy, multicast policy, TTL policy, or central SNAT map is used in an interface in version 7.4.5, 7.6.0, 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 7.6.1 or 7.6.2.<br><b>Workaround:</b> After upgrading to 7.6.1 or 7.6.2, users must manually recreate these policies and assign them to the appropriate SD-WAN zone. |
| 1106072 | The image file transfer between FortiManager and FortiGate may not work as expected when transferred by the FGFM tunnel.  |

## User & Authentication

| Bug ID  | Description   |
|---------|---|
| 1021719 | On the <i>System &gt; Certificates</i> page, the <i>Create Certificate</i> pane does not function as expected after creating a new certificate.   |
| 1082800 | When performing LDAP user searches from the GUI against LDAP servers with a large number of users (more than 100000), FortiGate may experience a performance issue and not operate as expected due to the HTTPSD process consuming too much memory. User may need to stop the HTTPSD process or perform a reboot to recover.<br><b>Workaround:</b> Perform an LDAP user search using the CLI. |

## VM

| Bug ID  | Description   |
|---------|---|
| 1146370 | AWS bootstrap is unable to parse IAM role profile properly due to the length. |

## Web Filter

| Bug ID  | Description   |
|---------|---|
| 1040147 | Options set in <code>ftgd-wf</code> cannot be undone for a web filter configuration.          |
| 1058007 | Web filter custom replacement messages in group configurations cannot be edited in FortiGate. |

## WiFi Controller

| Bug ID  | Description  |
|---------|--|
| 1083395 | In an HA environment with FortiAPs managed by primary FortiGate, the secondary FortiGate GUI <i>Managed FortiAP</i> page may show the FortiAP status as offline if the FortiAP traffic is not routed through the secondary FortiGate.<br>This is only a GUI issue and does not impact FortiAP operation. |

# Built-in AV Engine

AV Engine 7.00034 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

# Built-in IPS Engine

IPS Engine 7.01026 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© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.