



# Release Notes

FortiADC 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)



May 22, 2026

FortiADC 7.6.7 Release Notes

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>What's new</b> .....	<b>6</b>
System .....	6
Server Load Balance .....	6
Global Load Balance .....	6
Platform .....	7
<b>Hardware, VM, cloud platform, and browser support</b> .....	<b>8</b>
<b>Resolved issues</b> .....	<b>10</b>
<b>Known issues</b> .....	<b>12</b>
<b>Image checksums</b> .....	<b>13</b>
<b>Upgrade notes</b> .....	<b>14</b>
Supported upgrade paths .....	14
Data Partition Expansion 7.6.2 .....	15
Upgrading a stand-alone appliance .....	17
Upgrading an HA cluster .....	18
Special notes and suggestions .....	20

## Change Log

Date	Change Description
May 22, 2026	FortiADC 7.6.7 Release Notes initial release.

# Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.6.7, Build 0676.

To upgrade to FortiADC 7.6.7, see [Upgrade notes](#).

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: <https://docs.fortinet.com/product/fortiadc>.

# What's new

FortiADC 7.6.7 introduces enhancements and new features across various modules including Web Application Firewall, Server Load Balance, Global Load Balance, and more.

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

## System

### Certificate

#### **ACME External Account Binding (EAB) Support 7.6.7**

FortiADC now supports the Automated Certificate Management Environment (ACME) **External Account Binding (EAB)** protocol extension. While standard ACME typically only verifies domain ownership, EAB allows FortiADC to securely link its automated ACME client to existing, pre-registered accounts with commercial Certificate Authorities (CAs) such as DigiCert, ZeroSSL, or Sectigo. This ensures that only authorized clients can request certificates under a specific account profile, enabling organizations to utilize paid CA services, manage centralized billing, and enforce organizational validation (OV/EV) policies that are not available through standard free ACME services.

## Server Load Balance

#### **Stream Scripting Support for Session Persistence 7.6.7**

FortiADC 7.6.7 expands the capabilities of the Stream Scripting engine to include native session persistence management within **L7 TCP/UDP Virtual Servers**. Previously, using stream scripts and persistence together could lead to initialization conflicts where script logic would override standard persistence settings. This update resolves those conflicts by allowing the LB method, LB persistence, and Lua scripting modules to work in coordination. This introduces specialized Lua API commands and events that allow administrators to programmatically control how sessions are stored in and retrieved from the persistence table.

## Global Load Balance

#### **GLB Scalability for Multi-User Environments 7.6.7**

To improve multi-tenancy capabilities and support large-scale deployments, FortiADC 7.6.7 has standardized and increased the maximum configuration values for key Global Load Balancing (GLB) objects to **4096** across all platforms. Previously, these configuration limits varied depending on the hardware or virtual machine (VM) platform capacity. This update ensures uniform scalability and consistent performance for high-density environments regardless of the appliance model.

## Platform

### **OpenSSL Upgrade to 3.3.7 for Improved Security 7.6.7**

FortiADC 7.6.7 upgrades the OpenSSL library to version 3.3.7 to align with the latest security compliance requirements and upstream fixes.

## Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.6.7. All supported platforms are 64-bit version of the system.

### Supported Hardware:

- FortiADC 300D
- FortiADC 100F
- FortiADC 120F
- FortiADC 200F
- FortiADC 220F
- FortiADC 300F
- FortiADC 320F
- FortiADC 400F
- FortiADC 420F
- FortiADC 1200F
- FortiADC 2200F
- FortiADC 4200F
- FortiADC 5000F

For more information on the supported hardware models, see FortiADC's [Hardware Documents](#).

### VDOM capacity by FortiADC VM model

The following table lists the maximum number of supported VDOMs for each FortiADC VM model and the corresponding recommended system memory:

VM Model	Maximum VDOMs	Recommended System Memory
VM01	10	8 GB
VM02	10	8 GB
VM04	25	≥ 16 GB
VM08	45	≥ 32 GB
VM16	60	≥ 64 GB
VM32	90	≥ 128 GB
<b>VMUL</b>	<b>90</b>	<b>≥ 128 GB</b>

**Supported hypervisor versions:**

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0
Microsoft Hyper-V	Windows Server 2012 R2, 2016 and 2019
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5
OpenStack	Pike, Octavia 2023.2
Nutanix	AHV
Proxmox VE	6.4
Huawei FusionCompute	8.9.0

**Supported cloud platforms:**

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- OCI (Oracle Cloud Infrastructure) and OCI DRCC (Dedicated Region Cloud@Customer)
- Alibaba Cloud
- IBM Cloud

For more information on the supported cloud platforms, see the FortiADC [Private Cloud](#) and [Public Cloud](#) documents.

**Supported web browsers:**

- Mozilla Firefox version 109
- Google Chrome version 110

We strongly recommend you set either of the Web browsers as your default Web browser when working with FortiADC. You may also use other (versions of the) browsers, but you may encounter certain issues with FortiADC's Web GUI.

## Resolved issues

The following issues have been resolved in FortiADC 7.6.7 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
1286617	When executing a stream script using the LB:upstream or LB:set_peer functions, Layer 7 load balancing traffic is incorrectly routed to arbitrary real servers within a pool. This occurs when multiple real servers share an identical IP address but use different service ports, as the server selection mechanism fails to compare port numbers during configuration lookup.
1286214	Administrators cannot log in to the FortiADC GUI due to an HTTP 401 error, while CLI access remains functional. In high-density GSLB topologies, frequent Virtual Server status transitions generate an excessive volume of system log files, exhausting the storage capacity of the /tmp directory partition due to a lack of file rotation and size limit constraints.
1282339	Virtual IP (VIP) addresses remain bound to the kernel IP stack and continue responding to ICMP echo requests after their associated Virtual Server and NAT objects are disabled or deleted. This occurs when an IP address is shared simultaneously between a 1-to-1 NAT configuration and a Layer 4 or Layer 7 Virtual Server, as the address validation check fails to evaluate the operational status of matching objects before suppressing netlink IP removal commands.
1281066	The GUI Security widget continues to display Bot Detection (crawler) event statistics after a source IP exception has been configured. While the exception successfully suppresses the generation of new traffic logs, the security dashboard statistics module incorrectly bypasses the allowlist validation logic, counting matching traffic events despite the active exception.
1273070	Custom error pages embedded within an iframe display with truncated bottom content due to an unreliable iframe onload height calculation that fails to capture the full vertical dimension of the document.
1272167	SNMPv3 traps may fail to be processed by third-party monitoring tools (such as Zabbix) due to a lack of support for EngineID discovery through the <b>snmpFrameworkMIB</b> OID. Despite the EngineID being included in the trap packet, certain external management systems require this specific OID to establish the synchronization necessary for secure SNMPv3 communication.

Bug ID	Description
1271938	HTTP/HTTPS health checks configured with basic authentication credentials fail unexpectedly, causing functional real servers to be marked as down. This occurs when the backend server responds with an HTTP 401 Unauthorized status but omits the WWW-Authenticate header, preventing the health check daemon from executing its secondary credentialed probe.
1271727	In GLB topologies, SNMP queries tracking global Virtual Server status incorrectly return an Unknown string for generic server members. While the FortiADC GUI accurately reflects the active operational state of these backend resources, the SNMP monitoring subsystem fails to poll or mirror the member-specific status updates.
1265994	HTTP health checks using HTTP CONNECT (with Local CONNECT or Remote CONNECT) intermittently stopped functioning and caused elevated CPU utilization. This resulted from a data size mismatch between expected and received health check responses, which caused the health check process to hang and required a manual process restart to restore monitoring and traffic flow.
1263251	Attempts to create an aggregate interface failed with "System API error" or "Enslave failed" messages. This occurred because an interface previously involved in a failed VLAN assignment remained internally locked by the system, preventing it from being added as a slave to the new aggregate master.
1262109	Custom health check scripts failed to execute following a configuration restore or migration to a new platform. This was caused by a synchronization error between the primary configuration directory and the temporary execution environment ( <code>/tmp_hc_root</code> ), resulting in "No such file or directory" errors even when the scripts were present in the main file system.
1245170	The <code>config-sync</code> process intermittently reported "synconf fails" or "there was some errors in configuration" despite the settings successfully synchronizing between devices. This resulted from transient CLI execution failures during the merge process, where the system incorrectly flagged non-critical processing delays or configuration order mismatches as functional errors.

## Known issues

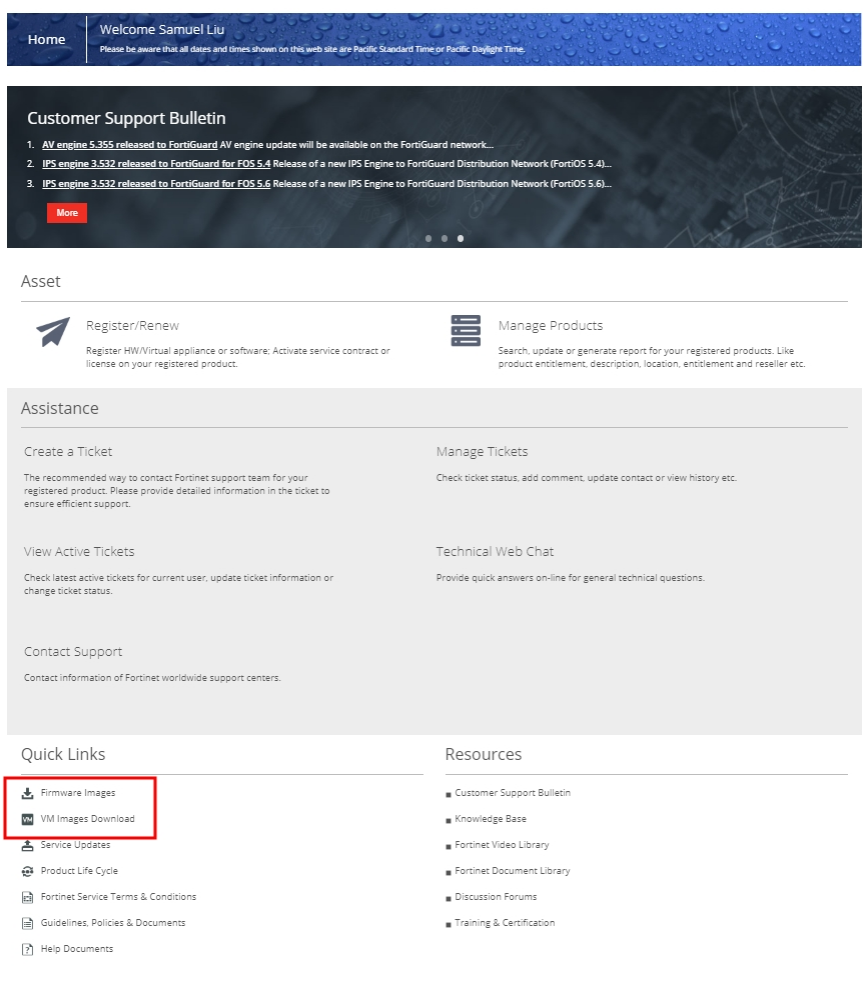
There are no known issues in version FortiADC 7.6.7.

# Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support contract.) In the File Name field, enter the firmware image file name including its extension, then click Get Checksum Code.

## Customer Service & Support image checksum tool



# Upgrade notes

This section includes upgrade information about FortiADC 7.6.7.

## Supported upgrade paths

To upgrade to FortiADC 7.6.7, you must proceed incrementally through each major version branch until you reach the target version. This ensures compatibility and system stability.

For example, to upgrade from **7.4.2** to **7.6.7**, follow this path:

7.4.2 → 7.4.x → **7.6.2** → 7.6.7

(Where "x" refers to the latest patch version in the branch.)

### **Important: Disk Expansion Requirement in 7.6.2**

If you are upgrading from **7.6.1 or earlier** and intend to upgrade to **7.6.3 or later**, you must first upgrade to **7.6.2**. This is required due to the disk expansion mechanism introduced in FortiADC 7.6.2.

Skipping 7.6.2 may result in system issues or failed upgrades due to incompatible disk layout changes. For details, see [Data Partition Expansion 7.6.2 on page 15](#).

### **7.6.2 to 7.6.3 or later**

Direct upgrade via the web GUI or the Console.

### **7.4.x to 7.6.0/7.6.1/7.6.2**

Direct upgrade via the web GUI or the Console.

### **7.2.x to 7.4.x**

Direct upgrade via the web GUI or the Console.

### **7.1.x to 7.2.x**

Direct upgrade via the web GUI or the Console.

### **7.0.x to 7.1.x**

Direct upgrade via the web GUI or the Console.

### **6.2.x to 7.0.x**

Direct upgrade via the web GUI or the Console.

### 6.1.x to 6.2.x

Direct upgrade via the web GUI or the Console.

### 6.0.x to 6.1.x

Direct upgrade via the web GUI or the Console.

### 5.4.x to 6.0.x

Direct upgrade via the web GUI or the Console.

### 5.3.x to 5.4.x

Direct upgrade via the web GUI or the Console.

### 5.2.x to 5.3.x

Direct upgrade via the web GUI or the Console.



For more information on upgrading from versions earlier than 5.2.x, please see the Upgrade Instructions document for that version.

## Data Partition Expansion - 7.6.2

In FortiADC 7.6.2, the data partition size is expanded to support larger firmware images and new feature implementations. The existing 200MB partition on most platforms has been a limiting factor for future enhancements. This update increases the partition size to the maximum allowable capacity based on the system's hardware, ensuring compatibility with upcoming releases.

This expansion applies only to hardware appliances and private cloud instances. Public cloud images will maintain the current partition size.

### Key Enhancements

Benefit	Details
<b>Increased Storage Capacity</b>	Expands the data partition from 200MB to the maximum available space on supported hardware and private cloud platforms, allowing more room for firmware images, logs, and feature enhancements.
<b>Seamless Future Upgrades</b>	Eliminates storage-related upgrade failures, ensuring smooth transitions to newer firmware versions.
<b>Enhanced System Longevity</b>	Prevents storage limitations from restricting feature adoption, extending the platform's scalability and maintainability.

## Upgrade Considerations and Limitations

Expanding the data partition in FortiADC 7.6.2 introduces specific upgrade requirements and operational impacts. Administrators must follow a structured upgrade path to ensure a smooth transition while considering potential limitations.

### Mandatory Upgrade Path

Upgrading beyond 7.6.2 (such as 7.6.3) requires installing 7.6.2 first. This ensures that the partition expansion is completed before applying a newer firmware version. Any attempt to upgrade directly to a post-7.6.2 release without first installing 7.6.2 will be blocked.

### Longer Upgrade Duration

Because the upgrade includes a partition resizing process, the total upgrade time is longer than a typical firmware update. The duration depends on the platform and storage configuration, so administrators should plan accordingly to minimize downtime.

### Irreversible Partition Change

Once the partition is expanded in 7.6.2, it cannot be reverted by downgrading to a previous firmware version. The partition remains in its expanded state even if an earlier release is installed. Before upgrading, ensure that your environment is compatible with 7.6.2 and later versions.

### HA Cluster Upgrade Best Practices

For HA (High Availability) clusters, follow these guidelines to prevent service disruption:

- Do not toggle HA mode during the upgrade, as this can lead to downtime for all nodes in the process.
- Upgrade each node individually, rather than upgrading all nodes at once, to minimize potential issues.
- For Active-Passive (A-P) clusters, start by upgrading the secondary node. Once the secondary node is fully operational, proceed to upgrade the primary node to ensure continued availability.

## Verifying Successful Data Partition Expansion

After performing an upgrade to FortiADC version 7.6.2 or later, the data partition will be expanded to provide increased storage capacity. To verify that the expansion has been successfully applied, you can use the following CLI command:

```
diagnose hardware get sysinfo partition
```

This command returns detailed information on the system's storage partitions, including the size of the data partition. By comparing the partition size values before and after the upgrade, you can confirm that the partition has been expanded as expected.

Example output comparison:

Platform	Before Upgrade to 7.6.2	After Upgrade to 7.6.2
Hardware (1200F)	<pre>FortiADC-1200F # diagnose hardware get sysinfo partition Disk /dev/sda: 240.0 GB, 240057409536 bytes 1 heads, 63 sectors/track, 7442256 cylinders Units = cylinders of 63 * 512 = 32256 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdal *            2      7442256  234431032+ 83 Linux Partition 1 does not end on cylinder boundary  Disk /dev/sdb: 2013 MB, 2013265920 bytes 1 heads, 62 sectors/track, 63421 cylinders Units = cylinders of 62 * 512 = 31744 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdb1 *            197           6649      200000    83 Linux Partition 1 does not end on cylinder boundary /dev/sdb2            6649       13100      200000    83 Linux Partition 2 does not end on cylinder boundary /dev/sdb3           13100       45358     1000000    83 Linux Partition 3 does not end on cylinder boundary</pre>	<pre>FortiADC-1200F # diagnose hardware get sysinfo partition Disk /dev/sda: 240.0 GB, 240057409536 bytes 1 heads, 63 sectors/track, 7442256 cylinders Units = cylinders of 63 * 512 = 32256 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdal *            2      7442256  234431032+ 83 Linux Partition 1 does not end on cylinder boundary  Disk /dev/sdb: 2013 MB, 2013265920 bytes 1 heads, 62 sectors/track, 63421 cylinders Units = cylinders of 62 * 512 = 31744 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdb1 *            197       13100      400000    83 Linux Partition 1 does not end on cylinder boundary /dev/sdb2 *           13100       26004      400000    83 Linux Partition 2 does not end on cylinder boundary /dev/sdb3            26004       58262     1000000    83 Linux Partition 3 does not end on cylinder boundary</pre>
Virtual Machine	<pre>FortiADC-VM # diagnose hardware get sysinfo partition Disk /dev/sda: 2147 MB, 2147483648 bytes 1 heads, 63 sectors/track, 66576 cylinders Units = cylinders of 63 * 512 = 32256 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdal *            194           6543      200000    83 Linux Partition 1 does not end on cylinder boundary /dev/sda2            6543       12892      200000    83 Linux Partition 2 does not end on cylinder boundary /dev/sda3           12892       25591      400000    83 Linux Partition 3 does not end on cylinder boundary  Disk /dev/sdb: 32.2 GB, 32212254720 bytes 1 heads, 63 sectors/track, 998643 cylinders Units = cylinders of 63 * 512 = 32256 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdb1 *            2      998644  31457248+ 83 Linux Partition 1 does not end on cylinder boundary</pre>	<pre>FortiADC-VM # diagnose hardware get sysinfo partition Disk /dev/sda: 2147 MB, 2147483648 bytes 1 heads, 63 sectors/track, 66576 cylinders Units = cylinders of 63 * 512 = 32256 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdal *            194       22416      700000    83 Linux Partition 1 does not end on cylinder boundary /dev/sda2 *           22416       44638      700000    83 Linux Partition 2 does not end on cylinder boundary /dev/sda3            44639       57337      400000    83 Linux Partition 3 does not end on cylinder boundary  Disk /dev/sdb: 32.2 GB, 32212254720 bytes 1 heads, 63 sectors/track, 998643 cylinders Units = cylinders of 63 * 512 = 32256 bytes  Device Boot      Start          End      Blocks  Id System /dev/sdb1 *            2      998644  31457248+ 83 Linux Partition 1 does not end on cylinder boundary</pre>

## Upgrading a stand-alone appliance

The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- Updates the firmware on the inactive partition and then makes it the active partition.
- Copies the firmware from the active partition, upgrades it, and installs it in place of the configuration on the inactive partition.

For example, if partition 1 is active, and you perform the upgrade procedure:

- Partition 2 is upgraded and becomes the active partition; partition 1 becomes the alternate partition.
- The configuration on partition 1 remains in place; it is copied, upgraded, and installed in place of the configuration on partition 2.

This is designed to preserve the working system state in the event the upgrade fails or is aborted.


Firmware			
Partition	Active	Last Upgrade	Firmware Version
1	Enable	Thu Jul 7 05:15:02 2022	FA-VMX-7.00.01-FW-build0022
2	Disable	Mon Jun 6 14:12:21 2022	FA-VMX-6.01.04-FW-build0140

[Boot Alternate Firmware](#)

### Before you begin:

- You must have super user permission (user admin) to upgrade firmware.
- Download the firmware file from the Fortinet Customer Service & Support website: <https://support.fortinet.com/>
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

### To update the firmware:

1. Go to **System > Settings**.
2. Click the **Maintenance** tab.
3. Scroll to the **Firmware** section.
4. Click **Upgrade Firmware** to locate and select the firmware file.
5. Click  to upload the firmware and reboot.  
The system replaces the firmware on the alternate partition and reboots. The alternate (upgraded) partition becomes the active, and the active becomes the alternate.
6. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

## Upgrading an HA cluster

The upgrade page includes an option to upgrade the firmware on all nodes in an HA cluster from the primary node.

The following chain of events occur when you use this option:

1. The primary node pushes the firmware image to the member nodes.
2. The primary node notifies the member nodes of the upgrade, and takes on their user traffic during the upgrade.
3. The upgrade command is run on the member nodes, the systems are rebooted, and the member nodes send the primary node an acknowledgment that the upgrade has been completed.
4. The upgrade command is run on the primary node, and it reboots. While the primary node is rebooting, a member node assumes the primary node status, and traffic fails over from the former primary node to the new primary node.


After the upgrade process is completed, the system determines whether the original node becomes the primary node, according to the HA Override settings:

- If Override is enabled, the cluster considers the Device Priority setting. Both nodes usually make a second failover in order to resume their original roles.
- If Override is disabled, the cluster considers the uptime first. The original primary node will have a smaller uptime due to the order of reboots during the firmware upgrade. Therefore, it will not resume its active role. Instead, the node with the greatest uptime will remain the new primary node. A second failover will not occur.

**Before you begin, do the following:**

1. Make sure that you have super user permission (user admin) on the appliance whose firmware you want to upgrade.
2. Download the firmware file from the Fortinet Customer Service & Support website:  
<https://support.fortinet.com/>
3. Back up your configuration before beginning this procedure. Reverting to an earlier version of the firmware could reset the settings that are not compatible with the new firmware.
4. Verify that the cluster node members are powered on and available on all of the network interfaces that you have configured. (Note: If required ports are not available, HA port monitoring could inadvertently trigger an additional failover, resulting in traffic interruption during the firmware update.)

**To update the firmware for an HA cluster:**

1. Log into the web UI of the *primary* node as the `admin` administrator.
2. Go to **System > Settings**.
3. Click the **Maintenance** tab.
4. Scroll to the **Upgrade Firmware** button.
5. Click **Choose File** to locate and select the file.
6. Enable the **HA Cluster Upgrade**.
7. Click  to upload the firmware and start the upgrade process.

After the new firmware has been installed, the system reboots.



When you update software, you are also updating the web UI. To ensure the web UI displays the updated pages correctly:

- Clear your browser cache.
- Refresh the page.

In most environments, press Ctrl+F5 to force the browser to get a new copy of the content from the web application. See the Wikipedia article on browser caching issues for a summary of tips for many environments:

[https://en.wikipedia.org/wiki/Wikipedia:Bypass\\_your\\_cache](https://en.wikipedia.org/wiki/Wikipedia:Bypass_your_cache).

---

## Special notes and suggestions

### 7.2.3

- The real server auto-populate feature is currently supported only in FortiADC version 7.2.3. Upgrading from version 7.2.3 to 7.4.0/7.4.1 will cause auto-populated real server related configuration loss, and may cause other unexpected behavior.  
Support for real server auto-population will be extended to later versions in the next release.

### 7.0.2/7.1.x

- After upgrading to 7.0.2/7.1.x, in Virtual Machine HA environments where both nodes have been installed with certificate embedded licenses you must reinstall those licenses. As some backend certificate files would have been synchronized and overwritten by the HA Peer (due to an existing bug), the certificate file would not be recoverable. Reinstalling the certificate embedded licenses is required to ensure they would work properly where they are needed, such as in ZTNA or FortiSandbox Cloud.

### 7.0.0

- When deploying the new GSLB based on FortiADC 7.0.0, the verify-CA function will be enabled by default.

### 6.2.2

- To use the SRIOV feature, users must deploy a new VM.

### 6.2.0

- In version 6.2.0, the default mode of QAT SSL has been changed to polling.

### 6.1.4

- Before downgrading from 6.1.4, ensure the new L7 TCP or L7 UDP application profiles are deleted or changed to a profile type that is supported in the downgrade version. Otherwise, this will cause the cmdb to crash.

### 5.2.0-5.2.4/5.3.0-5.3.1

- The backup configuration file in versions 5.2.0-5.2.4/5.3.0-5.3.1 containing the certificate configuration might not be restored properly (causing the configuration to be lost). After upgrading, please discard the old 5.2.x/5.3.x configuration file and back up the configuration file in the upgraded version again.



[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.