# Release Notes

## FortiADC 7.4.7

**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

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| March 5, 2025 | FortiADC 7.4.7 Release Notes initial release. |

# Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.4.7, Build 0387.

To upgrade to FortiADC 7.4.7, 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

FortiADC7.4.7 is a patch release, where no new features and enhancements are covered in this release.

# Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.4.7. All supported platforms are 64-bit version of the system.

**Supported Hardware:**

- FortiADC 300D
- FortiADC 400D
- FortiADC 100F
- FortiADC 120F
- FortiADC 200F
- FortiADC 220F
- FortiADC 300F
- FortiADC 320F
- FortiADC 400F
- FortiADC 420F
- FortiADC 1000F
- FortiADC 1200F
- FortiADC 2000F
- FortiADC 2200F
- FortiADC 4000F
- FortiADC 4200F
- FortiADC 5000F

For more information on the supported hardware models, see FortiADC's Hardware Documents.

**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 |
| Nutanix | AHV |
| Proxmox VE | 6.4 |

**Supported cloud platforms:**

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- OCI (Oracle Cloud Infrastructure)
- 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 7.4.7 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

| Bug ID | Description |
| --- | --- |
| 1128366 | Continuous IPS and AV packet processing can trigger a crash. |
| 1122921 | httpproxy crashes when processing XML files with malformed content. The issue occurs when Adaptive Learning or XML Protection functions (XML Limit Check, XML XSS Check, or SQL Injection Check) are enabled, and a malformed XML file is transferred. |
| 1122331 | REST API crashes when generating an all-in-one debug report. |
| 1120243 | FortiADC 1200F reports incorrect traffic and packet counter values in SNMP and CLI due to improper interface name handling, leading to discrepancies in monitoring data. |
| 1119257 | HA fails to establish between FortiADC nodes on firmware version 7.4.7 B0378 due to heartbeat message decoding errors, preventing synchronization between FortiADC-1 and FortiADC-2 KVM nodes. |
| 1118172 | GeoIP database upgrade fails if the version exceeds 256, causing manual import failures and HA secondary sync issues due to improper version validation. |
| 1116174 | An incorrect error message is triggered when upgrading from 7.4.x to a version beyond 7.6.2 without first upgrading to 7.6.2. |
| 1115210 | LDAP authentication fails over ConsolePort due to the admin_auth function not being invoked during login. |
| 1114401 | Request to increase maximum request header value length limit. |
| 1112914 | FortiADC attempts to connect to 8.8.8.8 on port 53 when the DNS is configured to 0.0.0.0, despite the DNS setting being invalid. |
| 1106109 | Connected route not displaying in HA-VRRP due to insufficient rtmd receiving buffer size configuration. |
| 1103348 | FortiADC AntiVirus does not block the EICAR file during upload (HTTP PUT), but can block it during download (HTTP GET) due to lack of support for scanning HTTP PUT traffic. |
| 1091639 | Local certificate import fails when the passphrase for the private key contains a backslash (), which is not handled properly. |
| 1091469 | Health check status is not properly updated on the secondary device after an HA failover. When the secondary device is promoted to primary, the status in the logical topology is not reflected correctly, leading to a lack of visibility on service availability and no alerts for service changes. |

# Known issues

There are no known issues in version FortiADC7.4.7.

# 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**
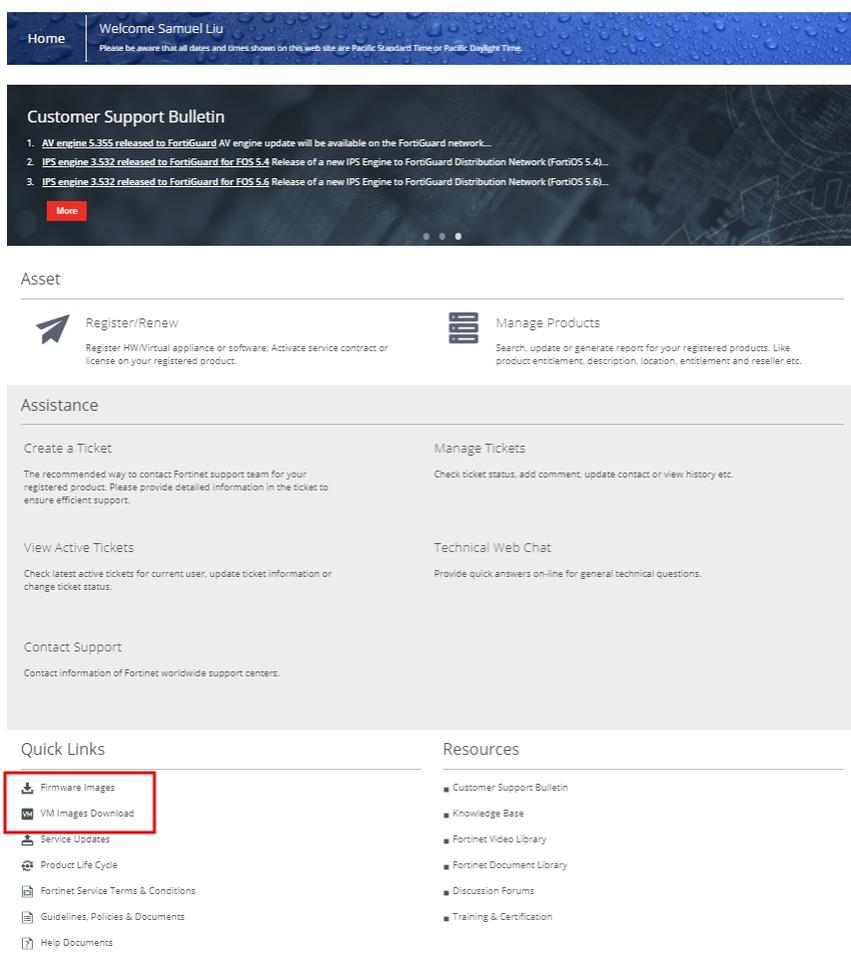
# Upgrade notes

This section includes upgrade information about FortiADC 7.4.7.

## Supported upgrade paths

This section discusses the general paths to upgrade FortiADC from previous releases.

If you are upgrading to a version that is in a higher version level, you will need to upgrade to the nearest branch of the major level incrementally until you reach the desired version. For example, to upgrade from 7.1.1 to 7.4.0, you will follow the upgrade path below:

7.1.1 → 7.1.x → 7.2.x → 7.4.0

(wherein "x" refers to the latest version of the branch)

### 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.

# 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 on 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.

| 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.)
5. 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 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.

# 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.

**FERTINET**

www.fortinet.com