Release Notes

FortiADC 8.0.2

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

TABLE OF CONTENTS

Change Log

Date	Change Description
December 12, 2025	FortiADC 8.0.2 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 8.0.2, Build 0056.

To upgrade to FortiADC 8.0.2, 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 8.0.2 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.

FortiAI

FortiAI Assistant for FortiADC 8.0.2

FortiADC 8.0.2 introduces FortiAI Assistant, an AI-powered assistant embedded directly in the FortiADC GUI. FortiAI Assistant enables administrators to use natural-language queries to obtain configuration guidance, inspect virtual server behavior, analyze system and security logs, and convert text-based prompts into Lua scripts through Text-to-Script. By allowing users to ask questions instead of manually navigating multiple pages or searching documentation, FortiAI Assistant streamlines common operational and troubleshooting workflows while keeping all configuration changes under administrator control.

Note: FortiAI Assistant availability depends on the FortiCare support level associated with the FortiADC license. VM licenses **without an active FortiCare support subscription** are not entitled to use FortiAI Assistant. FortiAI login is supported only when the license includes **Premium Support** or **Elite Support**.

Server Load Balance

Increased Capacity for Content Routing and Health Check Objects 8.0.2

FortiADC 8.0.2 increases the maximum number of Content Routing (CR) and Health Check (HC) objects that can be configured on the system. The increased limits allow administrators to define more CR and HC objects overall, improving scalability for complex traffic distribution and service monitoring scenarios. Existing constraints on how many health checks can be referenced by a single pool, and how many content routes can be referenced by a single virtual server, remain unchanged.

Network

VXLAN Support for Kubernetes Calico CNI 8.0.2

FortiADC 8.0.2 adds support for VXLAN-based networking with the Kubernetes Calico CNI, enabling FortiADC to integrate with Calico environments that use VXLAN for pod-to-pod and service traffic.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 8.0.2. 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 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, 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 8.0.2 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1226241	A system crash occurred under heavy DNS traffic on L4 UDP/TCP virtual servers using full NAT with a small SNAT pool. When the system attempted to allocate a local source port, most available ports were already in use, triggering excessive port-search loops and a resulting kernel soft lockup.
1224907	On the AWS platform, restoring a configuration file caused HA settings to be lost after reboot. The issue occurred because the HA **hb-type unicast** option was not parsed during the restore process.
1223551	On Hyper-V deployments, upgrading from 7.6.x to 8.0.0 or 8.0.1 caused the VM to lose its license after reboot.
1221882	In Advanced Bot Protection (ABP), JavaScript insertion failed when the HTML `<head>` tag included attributes (for example, `<head id="xxx">`). Only a plain `<head></head>` tag was recognized.
1220203	In Adaptive Learning, displaying a large number of URL entries could cause significant delays or GUI unresponsiveness due to the size of the data returned. Data transmission has been optimized to send large result sets in batches, improving page responsiveness when loading extensive AL statistics.
1219059	The GUI became inaccessible with a "Cannot allocate memory" error after long uptime. OSPF generated excessive error logs for virtual server IP addresses on bridge interfaces, filling the /tmp directory and preventing the GUI from loading.
1218158	Enabling compression on an L7 HTTPS virtual server together with `diagnose debug` for `httpproxy` caused the process to crash due to invalid data access in the debug-printing code.
1214530	After upgrade, some VDOMs showed inactive routes and all virtual servers in those VDOMs were down. `rtmd` did not receive interface address and link-status updates correctly when an interface IP overlapped with a load-balance IP pool, causing the routing state to be reported incorrectly.
1213980	In a VRRP Active-Active cluster, cloning a global DNS policy with a large number of A/AAAA records caused the primary node's Web GUI to hang and return "Bad Gateway" errors.
1212271	New CLI options are added to adjust the physical interface ring buffer size. Administrators can now configure `rxring` and `txring` values under `config system interface` and verify settings with the `diagnose hardware get deviceinfo nic-ringsize` command.

Bug ID	Description
1210252	Dynamic real server pools using the Kubernetes SDN connector failed to import members when large clusters were used. Duplicate node entries and command-size limits prevented real server and pool-member configuration from being saved, causing the pool to remain empty.
1208659	HA synchronization failed when an administrator account was changed to a global user while referencing a RADIUS server configured in a non-root VDOM. The mismatch prevented the configuration from applying on the primary node and caused HA sync to stop.
1205865	The `virtual-server-l2-cache-timeout` setting under `config router setting` did not take effect in non-root VDOMs. The value was treated as a global parameter, so only the root VDOM configuration was applied.
1198250	After upgrade, all L7 TCP virtual servers failed to start and returned RST packets. The `fnginx_new` process was not running because it could not bind to the virtual server IP address during startup, and its reload handling did not recover from the bind failure.
1049328	SNMP queries returned empty data for VLAN interfaces due to `ethtool` not reporting interface statistics.

Known issues

This section lists known issues in version FortiADC8.0.2, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1235192	When FortiAI returns content that includes Lua syntax or special characters, using the Copy icon may capture incorrect content. Selecting and copying the text manually avoids the issue.
1224892	Exporting large FortiAI chat histories as PNG or PDF may take more than 10 seconds and can fail in some cases. The issue is more likely to occur when the chat window is wide or the conversation is long. **Workaround**: Export the chat history as HTML instead. To avoid large exports, limit the number of queries in a single session.
1236224	In FortiAI text mode, some IPv6 addresses cannot be filtered in the log view, although they work correctly in Filter Mode.
1237045	When multiple browser windows are logged into FortiAI, a single chatbot session may use different FortiAI domains during interaction. This can cause the FortiAI server to return an invalid token and log the session out. **Workaround**: Refresh the page and re-login to the FortiAI assistant when the session disconnects.

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 8.0.2.

Supported upgrade paths

To upgrade to FortiADC 8.0.1, 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 **8.0.2**, follow this path:

7.4.2 → 7.4.x → **7.6.2** → 7.6.x → 8.0.2

(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 **8.0.0 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 .

7.6.2 to 8.0.x

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 8.0.2, 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
Increased Storage Capacity	Expands the data partition from 200MB to the maximum available space on supported hardware and private cloud platforms, allowing

Benefit	Details
	more room for firmware images, logs, and feature enhancements.
Seamless Future Upgrades	Eliminates storage-related upgrade failures, ensuring smooth transitions to newer firmware versions.
Enhanced System Longevity	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)		
Virtual Machine		

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.

Firmware			
⬆ Upgrade 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.

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.

FORTINET

www.fortinet.com