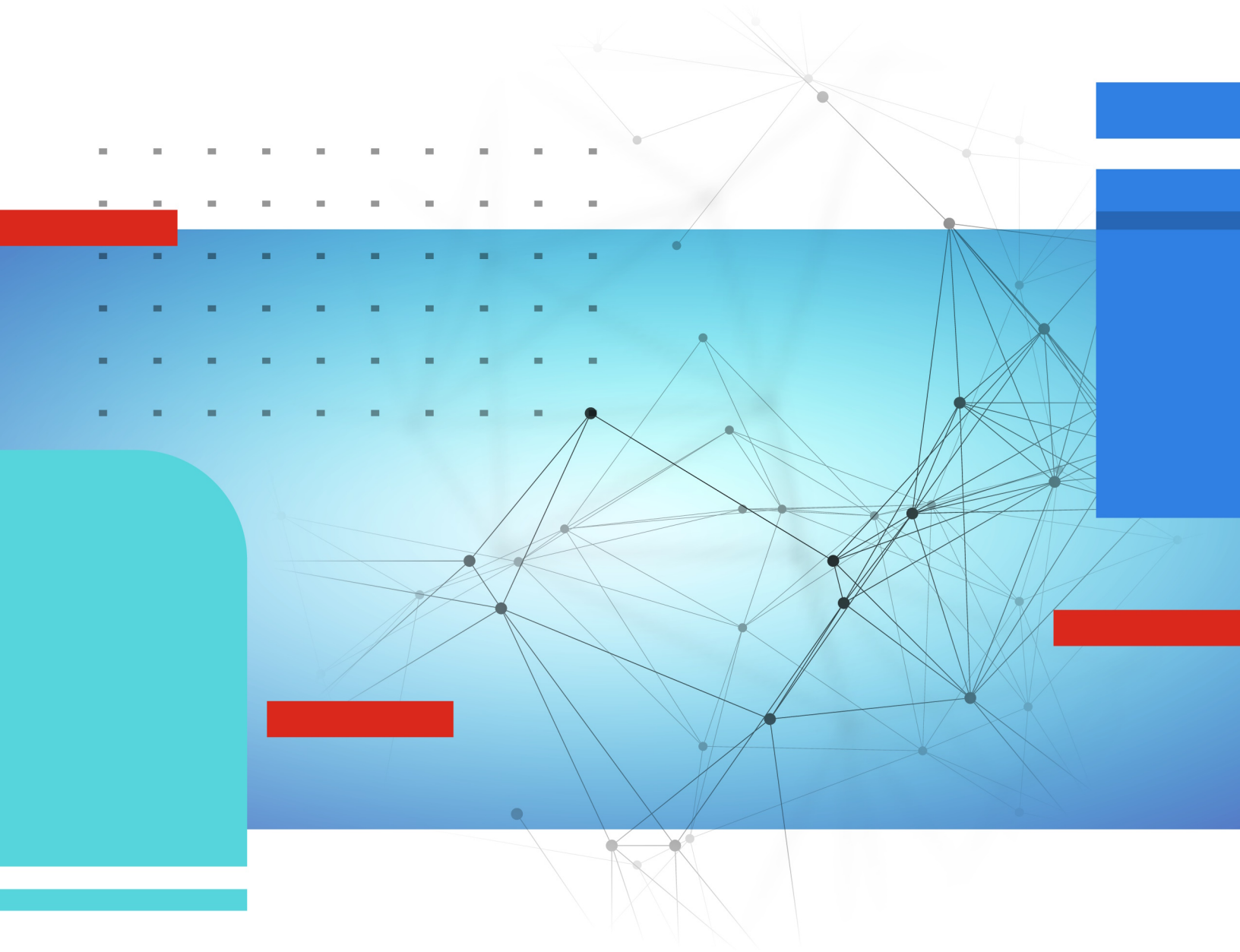
Release Notes

FortiADC 8.0.3



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

April 3, 2026
FortiADC 8.0.3 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
April 3, 2026	FortiADC 8.0.3 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 8.0.3, Build 0093.

To upgrade to FortiADC 8.0.3, 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 8.0.3 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 Log Analysis Enhancements 8.0.3

You can now use the **FortiAI Assistant** to perform deep-dive analysis on individual log entries for more granular operational and security insights. This update expands the assistant's capabilities to evaluate specific events within your traffic and security logs, transforming raw data into clear, actionable intelligence for faster troubleshooting and threat response.

Application Access Manager

Agentless Application Gateway New Features 8.0.3

Agentless Application Gateway (AAG) has been significantly enhanced to provide more flexible application delivery and granular access control:

- **SLB Virtual Server Integration**: AAG now leverages the full power of FortiADC by integrating the new WebAPP-Internal-Advanced bookmark type with SLB HTTP/S Virtual Servers. This enables enterprise-grade features such as WAF, advanced Load Balancing, Health Checks, and Scripting for bookmarked applications.
- **Shareable Bookmarks**: Bookmarks are now independent, shareable objects decoupled from App Groups. This allows for simplified object reuse and more efficient, centralized management across the platform.
- **User Group Matching**: The Authentication policy now supports **User Group Match** conditions. This allows administrators to define more granular access permissions based on specific user group memberships.
- **Unauthenticated URL Redirection**: For unauthenticated sessions, AAG now supports **URL auto-redirection**. This ensures a smoother user experience by automatically guiding users to the appropriate destination or login portal.

Web Application Firewall

WAF Signature Support for HTTP/3 and HTTP/2 8.0.3

FortiADC 8.0.3 now supports Web Application Firewall (WAF) Web Attack Signature scanning for HTTP/3 and HTTP/2 Virtual Servers. This update allows you to apply robust security policies to modern high-performance traffic, ensuring your services are protected against known web-based vulnerabilities.

RESTful API Input Security Check 8.0.3

You can now benefit from automated, deep-level security inspections for the FortiADC RESTful API to detect and prevent sophisticated exploits such as command injection and path traversal. FortiADC 8.0.3 introduces a specialized, independent signature database that performs real-time validation of API requests before business logic is executed. This feature ensures robust protection for the management interface by inspecting multiple input locations including headers, request bodies, query arguments, and URL paths without requiring any manual configuration.

Security Fabric

External ICAP Server Support 8.0.3

FortiADC 8.0.3 introduces support for external Internet Content Adaptation Protocol (ICAP) servers through a new Fabric Connector to provide an additional layer of file inspection. This feature allows FortiADC to act as an ICAP client, sending files to a third-party ICAP server for deep scanning after the local AntiVirus (AV) engine has performed its initial check. To use this feature, you enable ICAP scanning within an AntiVirus profile and associate it with a Virtual Server. If the ICAP server detects a threat, FortiADC automatically blocks the request and logs the event.

FortiSandbox Cloud Connectivity Enhancements 8.0.3

FortiADC 8.0.3 simplifies the integration with FortiSandbox by introducing an automated connection process and expanded regional support. These updates eliminate the need for manual account configuration, allowing the system to establish a secure link and retrieve available service regions automatically.

Server Load Balance

TLS 1.3 Hardening and Post-Quantum Cryptography Support 8.0.3

FortiADC 8.0.3 introduces advanced hardening for TLS 1.3 handshakes and adds support for Post-Quantum Cryptography (PQC) to protect data against future quantum computing threats. These enhancements provide granular control over cryptographic parameters through new security level settings and customizable signature and group selections.

FQDN Real Server DNS Cache and Refresh Configuration 8.0.3

FortiADC 8.0.3 introduces enhanced control over Domain Name System (DNS) resolution for Real Servers configured with Fully Qualified Domain Names (FQDN). This update allows you to manually configure the Time to Live (TTL) for cached DNS responses and define a minimum refresh interval, ensuring more predictable traffic steering when backend IP addresses change. By customizing these settings, you can prevent premature cache expiration or reduce the frequency of DNS queries to your nameservers.

Load Balance Pool Support in Stream Scripts 8.0.3

You can now use Stream Scripting to load balance an entire real server pool, instead of only individual real servers, by leveraging the new `LB:routing()` script command and Layer 7 content routing capabilities for non-

HTTP protocols. This enhancement allows scripts to inspect the application-layer payload and programmatically select a destination real server pool based on real-time traffic analysis.

Log & Report

Security Log GUI Redesign and Enhancements 8.0.3

Following the updates to the Traffic and Script logs, FortiADC 8.0.3 brings a complete redesign to the **Security Logs**. This update aligns the security interface with the modern, high-performance standard used across the platform while adding specialized investigation tools such as an **Analyze with AI button**, a **Log Details side panel**, and **one-click Policy Exceptions**.

Script Log Enhancement 8.0.3

Following the redesign of the Traffic Log interface in version 8.0.1, FortiADC 8.0.3 extends these modern GUI enhancements to the **Script Logs**. This update ensures a consistent user experience across different log types, aligning the Script Log interface with the streamlined, high-performance layout used for traffic analysis.

GUI

Enhanced User Interface and Workflow Reorganization 8.0.3

You can now navigate a more intuitive and streamlined management interface designed to enhance workflow efficiency and configuration consistency. FortiADC 8.0.3 introduces a large-scale reorganization of the management interface, refining navigation across the **System**, **Server Load Balance**, **Global Load Balance**, and **Web Application Firewall** menus. These updates simplify complex configurations, better align with policy creation flows, and centralize security-first settings for more efficient daily management.

Platform

OpenSSL Upgrade to 3.5 8.0.3

FortiADC 8.0.3 upgrades the OpenSSL library to version 3.5 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 8.0.3. 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 8.0.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
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.
1264125	Layer 7 TCP virtual servers using the `PERSIS_HASH_SRC_ADDR` persistence method experienced a rapid memory leak, leading to service instability and high memory utilization. This resulted from a failure to release memory during frequent virtual server configuration updates, which were triggered by unstable health check statuses.
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 (`/tmp_hc_root`), resulting in "No such file or directory" errors even when the scripts were present in the main file system.
1261741	In GLB FortiView, the host status appeared as "unknown" when the combined character length of the policy, hostname, and domain name exceeded 63. This resulted from an internal hash key truncation bug that incorrectly limited the lookup string to 64 characters instead of 512, though DNS query functionality remained unaffected.
1253275	FortiADC unexpectedly reset HTTP/HTTPS connections immediately after the client TCP SYN. This was caused by an internal load balancer process crash that occurred when inbound or outbound traffic limit values were set above 17,100,000. While the configuration was accepted by the CLI, the high value triggered a memory fault during traffic processing.
1249923	Enhanced the AAG by adding an **App Start In** parameter to Remote App bookmarks. This field allows administrators to define a specific working directory, ensuring successful connectivity for Microsoft RemoteApp services and other applications that require a defined "Start In" path to

Bug ID	Description
	launch.
1248712	FortiADC failed to validate licenses through the FortiFlex portal, resulting in an "authentication with registration servers" hang. This was caused by an intermittent SSL handshake failure during FortiGuard Distribution Service (FDS) communication, where a hostname mismatch occurred because the Server Name Indication (SNI) was not correctly aligned with the Anycast domain during certificate verification.
1245170	The `config-sync` 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.
1243690	Virtual servers using Lua scripts intermittently shared sensitive client data, such as certificate subject strings, across different user sessions. This occurred because variables declared at the global script scope are shared by all sessions handled by the same worker process. To ensure strict data isolation, session-specific data must be stored in a local scope or managed within a global table using unique session keys (such as client IP and port).
1243266	In Layer 7 TCP virtual server configurations, FortiADC incorrectly sent TCP resets (RST) immediately following the client SYN. This occurred due to an accumulation of abnormal fnginx worker processes triggered by repeated daemon crashes, or when virtual server names differed only by letter case, which caused configuration update failures during initialization.
1241536	FortiADC licenses were incorrectly detected as invalid after upgrading to v8.0.x on Hyper-V and Azure platforms. This resulted from a failure in the new system kernel to accurately identify the number of available vCPUs, causing a mismatch with the licensed resource limits. While trial licenses remained functional, full licenses appeared inactive until this resource-counting logic was corrected.
1240795	Enhanced the AAG Web APP bookmarks to support internal hostnames (FQDNs). This allows administrators to configure backend server destinations using domain names instead of being restricted to static IP addresses, ensuring compatibility with environments where backend services are only reachable via FQDN.
1238255	The SNMP OID for VDOM concurrent connections reported abnormal or excessively high values. This resulted from a synchronization mismatch where the internal VDOM connection counter was decreased multiple times upon session expiration, leading to an underflow and incorrect statistical output.
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.

Bug ID	Description
1236224	In FortiAI text mode, some IPv6 addresses cannot be filtered in the log view, although they work correctly in Filter Mode.
1235827	Input validation profiles failed to inspect parameters within decompressed traffic and caused system crashes. This resulted from an out-of-bounds memory write during the decompression process, which prevented security policy enforcement on subsequent application pages and led to CPU spikes and daemon instability.
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.
1232774	After upgrading to v7.4.8 on the FortiADC 300D, SLB servers in the GLB module failed to retrieve virtual server status when health check options were enabled. This resulted from a communication breakdown between the SLB and GLB modules, which prevented metadata synchronization for Virtual Server Pools and the FortiView Logical Topology.
1224441	FortiADC 1200F units with specific SSD models incorrectly reported an excessively high `Program_Fail_Count_Chip` value. This was a false positive caused by a reporting tool decoding error and did not indicate an actual hardware failure.
1222808	FortiADC sent unexpected, encrypted UDP packets to FortiManager on port 53 every few minutes. This occurred because the URL filter daemon initiated periodic availability checks to FortiGuard Distribution Servers (FDS) even when the Web Filter service was unlicensed and inactive.
1204472	FortiADC units experienced unexpected reboots due to a kernel crash. This resulted from an out-of-bounds memory access error during multipath route lookups, where the system attempted to access a non-existent index in the forwarding information base (FIB) array.
1133341	Enhanced FortiView to support manual termination of AAG user sessions. Administrators can now disconnect active AAG users directly from the User Session monitoring table to assist with access operations and session management.

Known issues

This section lists known issues in version FortiADC8.0.3, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

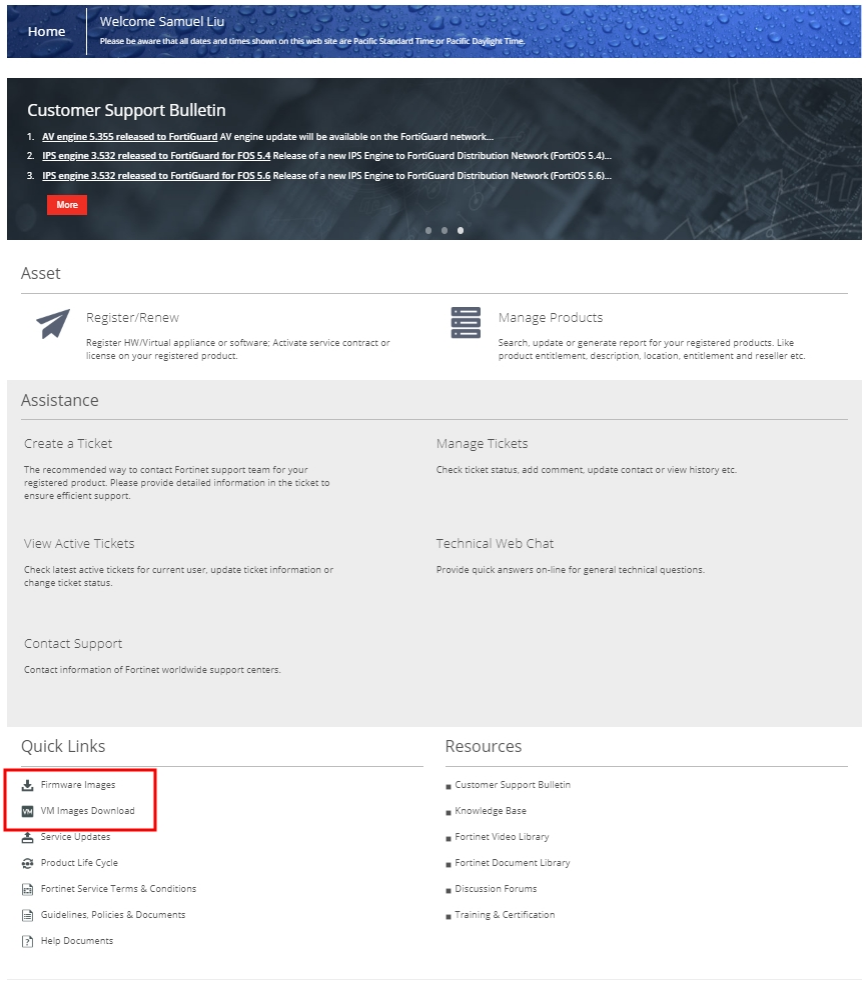
Bug ID	Description
1270576	The output of the CLI command `diagnose hardware get deviceinfo transceiver` incorrectly reports that no transceiver is detected when executed from a non-root VDOM. This is a display issue only; the physical SFP+ modules and interfaces function normally, and accurate status can still be verified via the root VDOM or shell-level diagnostics.
1272426	The **External URL** field in AAG Web APP Internal Advanced bookmarks does not support IPv6 address formats. This results from a regular expression (regex) limitation that prevents the system from correctly parsing and fetching rules when an IPv6 address is used instead of an IPv4 address or FQDN.
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.

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 8.0.3.

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 **8.0.3**, follow this path:

7.4.2 → 7.4.x → **7.6.2** → 7.6.x → 8.0.3

(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 Data Partition Expansion 7.6.2 on page 17.

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 8.0.3, 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.

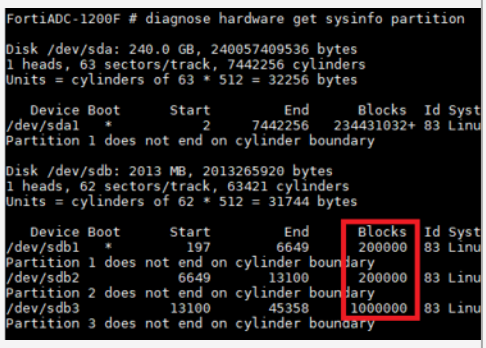
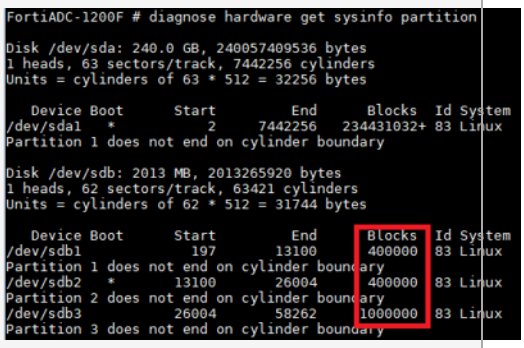
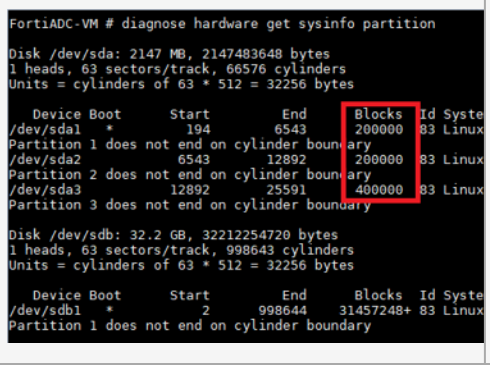
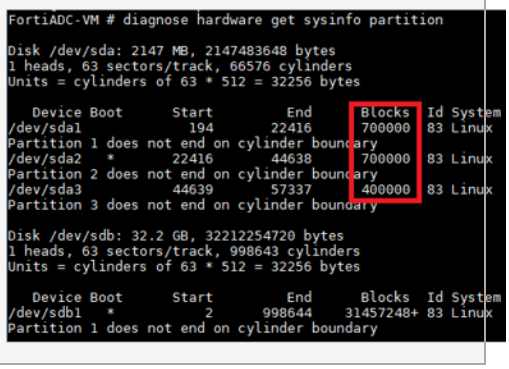
Verifying Successful Data Partition Expansion

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

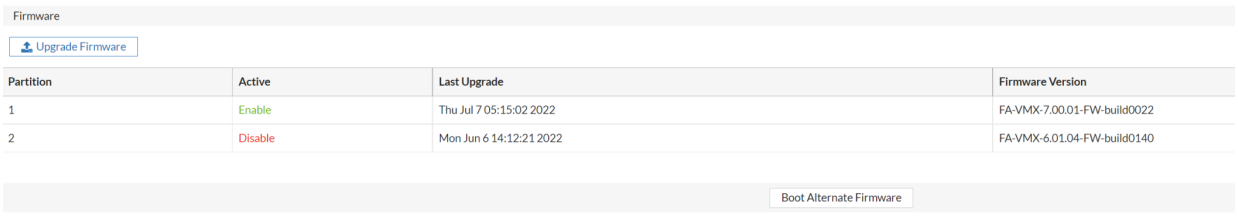
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- 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.



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

7.6.6

- **FortiADC 8.0.3 does not support the "Strip Domain From Username" feature introduced in version 7.6.6**. If you upgrade from version 7.6.6 to 8.0.3, existing **Strip Domain From Username** configurations within User Group members will be lost. This may cause authentication failures in environments that rely on domain stripping to route credentials to backend servers (such as LDAP, RADIUS, or Local) that do not recognize domain-qualified usernames (e.g., `domain\user`, `user@domain`, or `domain/user`).
  Support for Strip Domain From Username will be extended to later versions in the next release. If your environment requires domain stripping, it is recommended to remain on version 7.6.6.

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