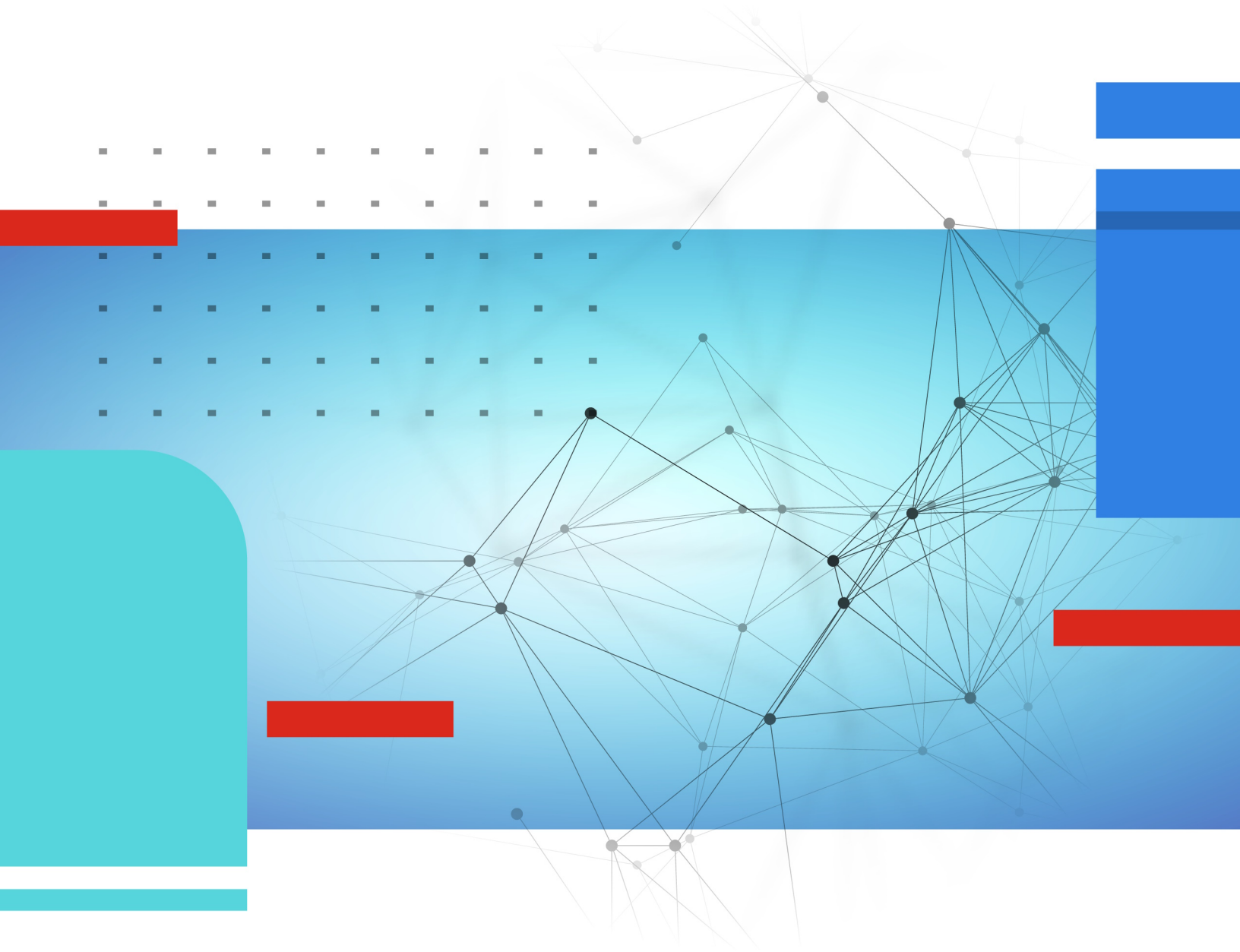
Release Notes

FortiADC 8.0.1



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

October 13, 2025
FortiADC 8.0.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
October 13, 2025	FortiADC 8.0.1 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 8.0.1, Build 0038.

To upgrade to FortiADC 8.0.1, 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 8.0.1 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.

Application Access Manager

Agentless Application Gateway New Features 8.0.1

FortiADC 8.0.1 introduces major new features to the Agentless Application Gateway (AAG), expanding its capabilities to publish internal web applications, enforce multi-factor authentication (MFA) at App Portal login, and improve portal usability with automatic language detection and customizable bookmark icons. These updates extend AAG to support browser-based access to internal resources such as intranet sites and collaboration platforms, providing secure, policy-driven delivery without the need for VPN software or client agents.

Security Fabric

Cisco ACI External Connector 8.0.1

FortiADC now supports direct integration with **Cisco ACI 5.2** through a new **Cisco ACI SDN** connector in the **Security Fabric > External Connectors** framework.

This connector establishes a northbound API connection to the Cisco Application Policy Infrastructure Controller (APIC), enabling FortiADC to automatically discover and synchronize ACI tenants, application profiles, and endpoint groups (EPGs) with its own load-balancing configuration.

By linking the application-centric visibility of Cisco ACI with FortiADC's traffic management engine, this feature delivers adaptive, SDN-driven load balancing that evolves automatically with your data-center topology.

FortiGate Security Fabric-Based Admin SSO 8.0.1

FortiADC now supports administrator Single Sign-On (SSO) through **FortiGate Security Fabric integration**. When connected to the Security Fabric where FortiGate acts as the root, FortiADC can use the FortiGate as its **SAML Identity Provider (IdP)** for administrator authentication.

System

WAF Signature Staging 8.0.1

FortiADC introduces support for **WAF Signature Staging**, providing a controlled process to evaluate newly released or modified FortiGuard attack signatures before they are enforced. With this capability, newly added or

updated signatures are first placed in a **Signature Staging** list. Administrators can monitor these signatures as they trigger on live traffic and review their Matched status before deciding whether to apply or disable them—reducing false positives and smoothing production rollouts. This capability is supported with **WAF Signature Database version 1.00063 and later**.

Disable Default Admin Account via CLI 8.0.1

Administrators now have the option to disable the built-in **admin** account using the new CLI command `set default-admin` under `config system global`. This enhancement improves security and compliance by allowing organizations to prevent login with the default account once alternate administrator accounts have been created. When disabled, the admin account cannot log in, and any active sessions are immediately terminated.

Socket Selection Hash Control via CLI 8.0.1

FortiADC introduces a new CLI option, `sip-to-same-sock`, under `config system global` to control how sessions are hashed across sockets. By default, sessions with the same source IP, destination IP, and destination port (`sip+dip+dport`) are consistently directed to the same CPU, `httproxy` process, and listening socket. This ensures that related sessions remain on the same processing path.

Server Load Balance

Advanced mTLS Support with Enhanced Client Authentication and C3D 8.0.1

FortiADC expands its **mutual TLS (mTLS)** capabilities with advanced features that strengthen security and improve deployment flexibility. mTLS requires both the client and server to authenticate each other using certificates, ensuring trusted, bidirectional communication.

While FortiADC already supported basic mTLS, this release introduces advanced functions for greater control and interoperability:

- **Enhanced Client Authentication** – Configurable authentication frequency and selective advertisement of trusted certificate authorities (CAs).
- **Client Certificate Constrained Delegation (C3D)** – Allows FortiADC to issue delegated client certificates when forwarding traffic to backend servers, maintaining mutual TLS authentication while still enabling SSL decryption and inspection.

Together, these enhancements provide administrators with fine-grained control over certificate handling, ensuring secure, verifiable mTLS chains on both the client- and server-facing sides of FortiADC.

Advanced TCP Optimization and Transparent Proxy Support for L7 TCP Virtual Servers 8.0.1

FortiADC extends its L7 TCP virtual server capabilities with support for transparent TCP proxying and advanced TCP optimization features. While transparent proxy modes (Layer 2 and Layer 3) were already available for other types of virtual servers, this enhancement makes them available for **L7 TCP virtual servers**, enabling inline deployments with full application-layer visibility and control. In addition, L7 TCP profiles now include per-connection tuning parameters and congestion control options, giving administrators precise control over throughput, efficiency, and reliability.

Content Rewriting support for HTTP/3 and Backend HTTP/2 8.0.1

FortiADC 8.0.1 extends the content rewriting functionality to HTTPS Virtual Servers that have HTTP/3 enabled on the frontend or Backend HTTP/2 enabled. Previously, content rewriting was limited to Virtual Servers with HTTP profiles, which meant services delivered over HTTP/3 or full end-to-end HTTP/2 could not take advantage of the same traffic manipulation policies.

Global Load Balance

New Secondary Zone Type with Secure AXFR Synchronization via TSIG Authentication 8.0.1

FortiADC introduces a new **Secondary zone type** to expand its DNS role beyond primary-only operation. Previously, FortiADC could act only as a primary DNS server, serving zone data to other secondaries. With this enhancement, it can also function as a secondary, synchronizing its DNS zone data from an upstream primary server using **AXFR (Authoritative Zone Transfer)**. To enable secure synchronization, this release also adds support for **TSIG (Transaction SIGnature) authentication**, ensuring that AXFR transfers and NOTIFY messages are validated and accepted only from trusted servers. Together, these enhancements provide a more flexible, interoperable, and secure foundation for Global Server Load Balancing (GSLB).

User-Defined Certificates and CA Verification for GSLB 8.0.1

FortiADC now supports user-defined certificates and peer certificate verification for Global Server Load Balancing (GSLB). This enhancement strengthens authentication between GLB and SLB, mitigates man-in-the-middle (MITM) risks, and enables integration with enterprise PKI infrastructures. It also extends cipher suite support to include FIPS-compliant options, ensuring compliance with stricter security requirements.

Network Security

CLI Commands to Manage TCP DoS Block List 8.0.1

FortiADC introduces two new CLI commands to manage entries in the TCP DoS block list:

- `execute dos get tcp-block-list` displays source IPs currently blocked by a DoS profile, along with source port, destination, and remaining block time.
- `execute dos release tcp-block-list` removes entries from the block list, either by source IP or all at once.

These commands apply specifically to **Layer 4 DoS protections** that use the **Period Block** action, including **TCP access flood protection** and **TCP slow-data attack protection**. When these protections detect excessive or abnormal connection behavior, offending source IPs are temporarily blocked for the configured duration.

Log & Report

Traffic Log Enhancement 8.0.1

The **Traffic Log** page has been completely redesigned to make log investigation faster, more flexible, and more intuitive. The new interface enables administrators to analyze large datasets without interruption, quickly isolate

events using dynamic filters, and customize the log view to focus on the most relevant metrics. These enhancements streamline routine monitoring and accelerate troubleshooting across all traffic log types.

Platform

Expanded Local Certificate Group Member Limit 8.0.1

FortiADC 8.0.1 increases the maximum number of Local Certificate Group Members from 256 to 1024. This change provides greater flexibility for large-scale deployments that manage extensive sets of local certificates within a single group.

OpenSSL Upgrade to 3.3 8.0.1

FortiADC 8.0.1 upgrades the OpenSSL library to version 3.3 to align with the latest security compliance requirements and upstream fixes.

OCI DRCC support 8.0.1

FortiADC-VM is supported in OCI Dedicated Region Cloud@Customer (DRCC). For more information, see Dedicated Region Cloud@Customer.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 8.0.1. 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

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 8.0.1 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1205106	In the GUI, the **Add Filter** option **under Network Security > Firewall** was incorrectly grayed out and unavailable.
1200598	When HTTPS service was enabled on port2 and port3 in an Active-Active HA cluster, a node could drop out of the cluster due to a GLB process binding failure during HA synchronization. The issue caused temporary cluster instability until the node rejoined.
1194018	After upgrading to version 7.4.8, external connections could experience performance degradation due to dropped packets on the ingress ADC. The issue was caused by an incorrect check in the LRO/GRO handling logic that required TSO to be enabled, resulting in packet drops when receiving large packets assembled by LRO/GRO.
1192054	Maximum Request Header Value Length limit increased to 16,384.
1191529	Editing a virtual server in AP mode failed with a “traffic group conflict” error because traffic group validation was incorrectly applied outside HA VRRP mode.
1190857	Virtual servers experienced timeouts and connection failures due to reverse routing lookups failing after fast forwarding entries expired.
1187948	Certificate configurations were lost after upgrade from 7.4.5 to 7.4.7 because private key passwords containing unescaped double quotes or backslashes caused configuration errors in CMDB.
1184789	FortiSandbox Cloud activation failed through a proxy with “FortiCloud internal error” due to an SSL read timing issue when responses were not received in time.
1184197	FortiADC licensed through FortiFlex remained restricted to VM01 limits despite valid VM08 entitlement due to incorrect CMDB tablesize handling after CPU allocation.
1178580	In Kubernetes environments using the FortiADC Ingress Controller, the SLB virtual server configuration in the GUI displayed an incorrect real server pool reference. When content routing was enabled, the associated real server pool field should have been hidden or disabled, as routing decisions were determined by content rules. The CLI configuration was unaffected.
1168921	After upgrading to firmware version 7.6.2, IPv6 routes are missing and the default route becomes inactive due to delayed initialization of `rtmd`, which

Bug ID	Description
	fails to load global address information during startup.
1168495	The system incorrectly counted SMTP (secure) and Diameter (SSL) services toward the hardware SSL instance limit. The limitation now correctly applies only to HTTPS and TCPS virtual servers.
1165214	In AAG authentication, passwords containing special characters were incorrectly URL-encoded, causing login failures for both local and remote user accounts. The issue has been corrected so that special characters are now processed properly. The characters \, ', and " remain unsupported, consistent with non-AAG local user password limitations.
1163215	DNS zone transfers fail through FortiADC when the zone file is large, as the system sends a TCP RST to the backend after partial transfer (~25,000 records), due to an insufficient backend receive buffer size.
1160460	SCEP certificate retrieval fails when the server returns a full certificate chain containing multiple certificates.
1153978	The FortiView real server pool statistics page did not display or allow selection of a time span for the traffic graph, unlike other FortiView views.
1150240	FortiADC (secondary) enters a reboot loop when connected to the network with the heartbeat interface active, triggered by a buffer overflow caused by an excessively long certificate file name.

Known issues

This section lists known issues in version FortiADC8.0.1, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

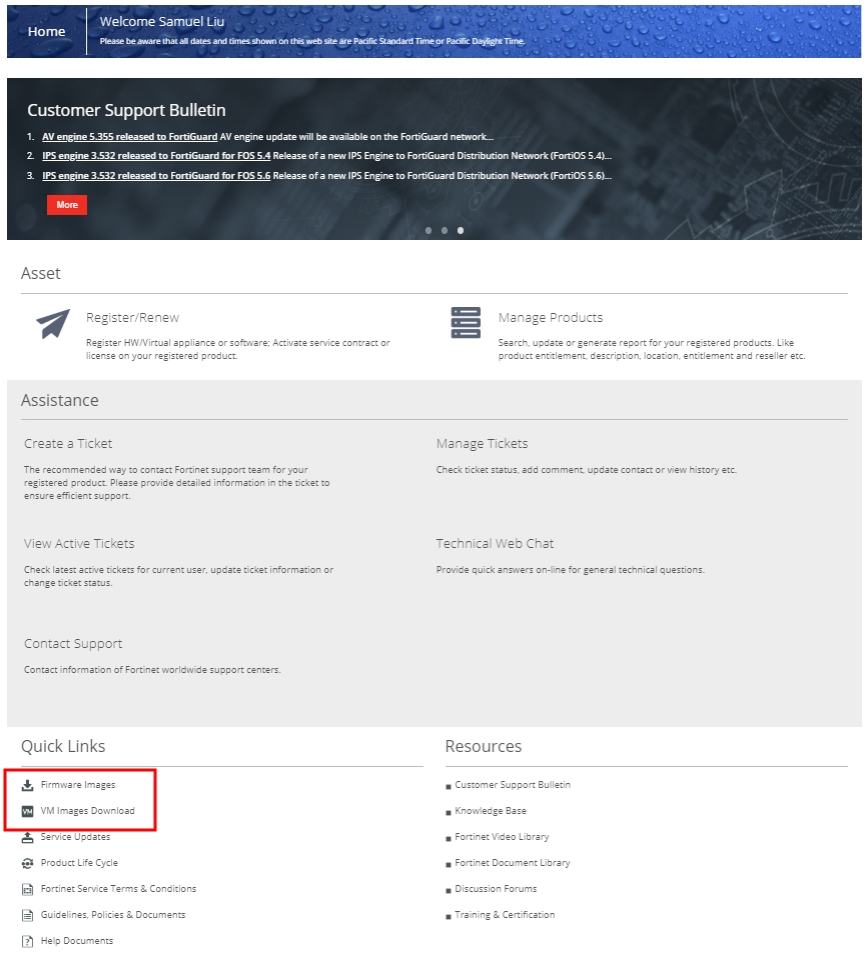
Bug ID	Description
1211495	After the default-admin account was disabled, the FortiADC Manager Connector could become non-functional and fail to send data to FortiADC Manager.

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 8.0.1.

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 **8.0.1**, follow this path:

7.4.2 → 7.4.x → **7.6.2** → 7.6.x → 8.0.1

(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 8.0.1, 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.

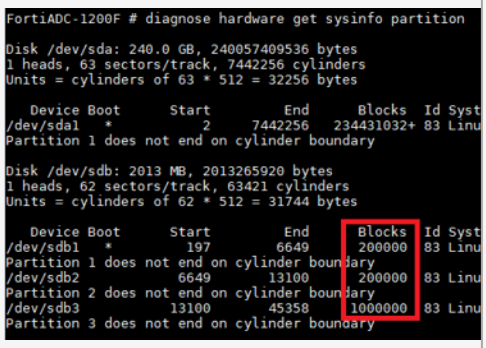
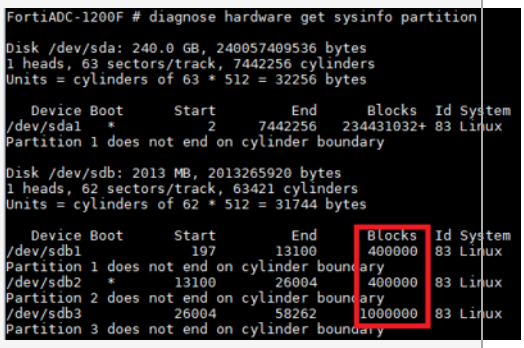
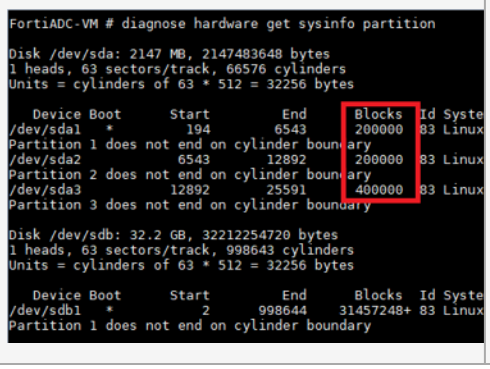
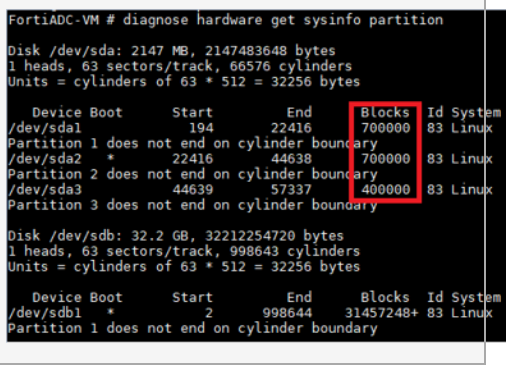
Verifying Successful Data Partition Expansion

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

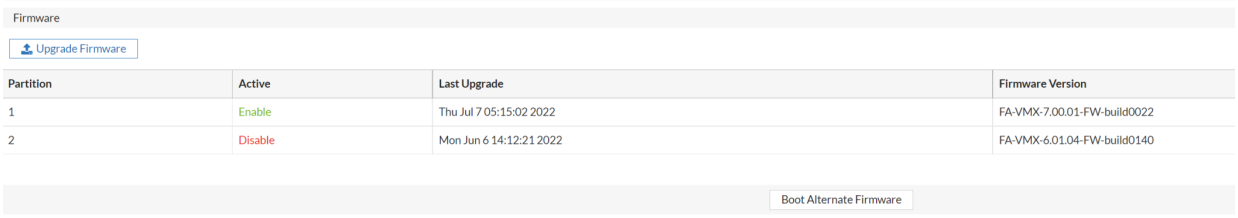
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- 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

7.2.3

- 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