

Release Notes

FortiADC 7.2.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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 CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 14, 2023

FortiADC 7.2.1 Release Notes

01-544-677187-20230414

TABLE OF CONTENTS

Change Log	4
Introduction	5
What's new	6
Hardware, VM, cloud platform, and browser support	7
Resolved issues	9
Known issues	12
Image checksums	13
Upgrade notes	14
Supported upgrade paths	14
Upgrading a stand-alone appliance	15
Upgrading an HA cluster	16
Special notes and suggestions	17

Change Log

Date	Change Description
April 14, 2023	FortiADC 7.2.1 Release Notes initial release.
June 8, 2023	Added ESXi 8.0 to supported hypervisor versions.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.2.1, Build 0220.

To upgrade to FortiADC 7.2.1, 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 7.2.1 offers the following new features:

Source IP support in L2 exception list/SSLi Bypass

- The L2 SSL Forward Proxy VS can now be bypassed based on either Destination IP or Source IP in the L2 Exception List Rule.
- In SSLi mode, the instance can now be bypassed based on either Destination IP or Source IP in the SSLi Bypass Rule.

Debug file download enhancements

- New file download option that allows you to download a text file that only contains the file names from `/var/log/crash/*`, instead of downloading the crash package that contains all the debug files.
- Concurrent requests will now be blocked to allow the current process to finish before running the next request.
- You can now terminate a debug file save request in progress.
- The SN.txt file will now include the FortiADC version information and serial number.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.2.1. 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 400F
- 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

Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)

- OCI (Oracle Cloud Infrastructure)
- Alibaba Cloud

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

Supported web browsers:

- Mozilla Firefox version 59
- Google Chrome version 65

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 7.2.1 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0903331	In the CORS Protection Rule list, cannot configure the request URL as a regular expression.
0897894	The FortiADC secondary unit becomes stuck in a reboot loop only when the network cable is connected. This occurs when the VLAN interface is set as the management interface instead of on the bonding interface. When the bonding interface is released before the VLAN interface, it will automatically trigger the release of the VLAN interface. However, if the VLAN interface is set as the management interface and holds a reference to the VLAN interface, it will prevent the VLAN interface from being released, leading to a system crash.
0897015	GUI: Unexpected errors occur when configuring NAT Source.
0892711	The FortiToken that FortiADC sends to the FortiToken Cloud server for MFA needs to be updated.
0891664	The customized form based authentication page cannot support domain names longer than 32 bytes, which results in redirection to an incomplete domain name.
0890333	Named service crashes when there is a configuration conflict.
0885150	Shared memory related crash caused by conflict between httpoxy and cmdb when cmdb reinit shared memory.
0884045	Firewall Policy deny logs are not generated when the packet is for Layer 4 virtual servers.
0883985	FortiADC Layer 2 forward proxy in transparent mode does not work well.
0883108	Secondary HA unit reload loop caused by the comment field of the alert policy becoming mismatched between the secondary and primary units when the comment defaults to <code>comment</code> in the primary after cmdb inits.
0882565	Typos in the upgrade completion message for the statistics database.
0882524	Unable to trigger FortiGate IP Ban action despite meeting configured conditions for the Automation stitch.
0881798	FQDN issue caused by longer self-generated keys. Require support for 2048 bits key size for both KSK and ZSK with the RSASHA256 algorithm.
0881065	Request to increase the Maximum Packet Count in Packet Capture from the current 10,000 to 100,000.
0879016	GUI: The warning message for admin password conformation rules should

Bug ID	Description
	not show for REST API admin.
0878735	GUI: Unable to save the parent Automation Trigger configuration and create the Alert Metric Expire Member child configuration on the same page.
0877361	No debug for incoming HTTP requests to the management interface web server.
0877061	GUI: An empty message box appears after saving FortiGSLB connector configuration.
0875877	ISC crashes when the host has more than two pools.
0875825	GUI: Does not exit configuration dialog automatically by clicking "Save" when configuring Member for MD5 Key List.
0875812	When using FSA/FSA cloud, uploading a file larger than 1.3 MB (oversized) causes the AV logs to report "AV engine meet error: archive corrupted".
0874263	GUI: When editing an existing Interface configuration, the Virtual Domain option should be greyed out.
0870372	FortiADC crashes and HA-failover was not triggered.
0859571	PPPoE not functioning on physical interface.
0858336	CORS Protection deny access even for legitimate traffic specified in Allowed Origin.
0853552	OCI performance issues resolved by adding irqbalance for virtIO in OCI.
0821545	GCP FortiADC marketplace only allows VMs with 1 VNIC deployment.

Common Vulnerabilities and Exposures

For more information, visit <https://www.fortiguard.com/psirt>.

Bug ID	Description
0896047/ 0896046/ 0896044/ 0896043/ 0896041/ 0896037/ 0896036/	FortiADC 7.2.1 is no longer vulnerable to the following CVE-Reference: CWE-120: Buffer Copy without Checking Size of Input ("Classic Buffer Overflow").
0892671/ 0891282/ 0891281/ 0891280/ 0887733/ 0838131	FortiADC 7.2.1 is no longer vulnerable to the following CVE-Reference: CWE-78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection").
0891392/ 0884844	FortiADC 7.2.1 is no longer vulnerable to the following CVE-Reference: CWE-1395: The product has a dependency on a third-party component that contains one or more known vulnerabilities.
0891336	FortiADC 7.2.1 is no longer vulnerable to the following CVE-Reference: CWE-23: Relative Path Traversal.

Bug ID	Description
0882586	FortiADC 7.2.1 is no longer vulnerable to the following CVE-Reference: CVE-2023-0286, CVE-2022-4304, CVE-2022-4203, CVE-2023-0215, CVE-2022-4450, CVE-2023-0216, CVE-2023-0217, CVE-2023-0401.
0874383	FortiADC 7.2.1 is no longer vulnerable to the following CVE-Reference: CVE-2022-42898.
0864662	FortiADC 7.2.1 is no longer vulnerable to the following CVE-Reference: CVE-2022-40303, CVE-2022-40304.

Known issues

This section lists known issues in version FortiADC 7.2.1, but may not be a complete list. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0900830	After the automation rule is triggered for a long time, the memory usage may not be recycled. This may happen when a vast number of logs are triggered by automation rules and the action takes a long time to be completed.
0898316	Apply-to-All-CORS-Traffic should only take effect with HTTP requests with header "Origin".
0885240/0884177	Due to FortiGate Cloud portal upgrade, statistics from FortiADC boxes can not be shown on their Sandbox portal.
0881992	Request for L7 DNS SLB to support forwarding of all DNS responses.
0875797	For the server-load-balance L7 virtual-server type explicit_http, the resolve host responds with incorrect IP address at certain condition.
0859565	After executing factory reset, the console shows the message indicating that the "bind failed" due to the address already being in use.
0838441	The same IP address can be configured on two different interfaces, with one being the static IP and the other from PPPoE.
0835874	Should be able to control minimal-responses to enhance named performance.

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

The screenshot shows the Fortinet Customer Service & Support portal. At the top, a blue banner displays 'Home' and 'Welcome Samuel Liu' with a note about time zones. Below this is a 'Customer Support Bulletin' section with three items: 'AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...', 'IPS engine 3.532 released to FortiGuard for FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...', and 'IPS engine 3.532 released to FortiGuard for FDS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...'. A 'More' button is visible. The main content area is divided into 'Asset' and 'Assistance' sections. 'Asset' includes 'Register/Renew' and 'Manage Products'. 'Assistance' includes 'Create a Ticket', 'Manage Tickets', 'View Active Tickets', 'Technical Web Chat', and 'Contact Support'. At the bottom, there are 'Quick Links' and 'Resources' sections. In the 'Quick Links' section, 'Firmware Images' and 'VM Images Download' are highlighted with a red box. The 'Resources' section lists various support resources like 'Customer Support Bulletin', 'Knowledge Base', 'Fortinet Video Library', 'Fortinet Document Library', 'Discussion Forums', and 'Training & Certification'.

Home Welcome Samuel Liu
Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time.

Customer Support Bulletin

1. AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...
2. IPS engine 3.532 released to FortiGuard for FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FDS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...

More

Asset

Register/Renew
Register HW/Virtual appliance or software; Activate service contract or license on your registered product.

Manage Products
Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

Assistance

Create a Ticket
The recommended way to contact Fortinet support team for your registered product. Please provide detailed information in the ticket to ensure efficient support.

Manage Tickets
Check ticket status, add comment, update contact or view history etc.

View Active Tickets
Check latest active tickets for current user; update ticket information or change ticket status.

Technical Web Chat
Provide quick answers on-line for general technical questions.

Contact Support
Contact information of Fortinet worldwide support centers.

Quick Links

- Firmware Images
- VM Images Download
- Service Updates
- Product Life Cycle
- Fortinet Service Terms & Conditions
- Guidelines, Policies & Documents
- Help Documents

Resources

- Customer Support Bulletin
- Knowledge Base
- Fortinet Video Library
- Fortinet Document Library
- Discussion Forums
- Training & Certification

Upgrade notes

This section includes upgrade information about FortiADC 7.2.1.

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 5.3.5 to 6.1.5, you will follow the upgrade path below:

5.3.5 → 5.4.x → 6.0.x → 6.1.5

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

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.


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.)
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

7.2.1

- Keep the old SSL version predefined configuration to ensure a smooth upgrade.

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

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.