



FortiADC - Release Notes

Version 7.0.1

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>

NSE 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



March 25, 2022

FortiADC 7.0.1 Release Notes

01-544-677187-20201112

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	11
Image checksums	12
Upgrade notes	13
Supported upgrade paths	13
Upgrading a stand-alone appliance from 4.2.x or later	16
Upgrading an HA cluster from 4.3.x or later	17
Special notes	19

Change Log

Date	Change Description
March 25, 2022	FortiADC 7.0.1 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.0.1, Build 0022.

To upgrade to FortiADC 7.0.1, see [Upgrade notes](#).

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: <http://docs.fortinet.com/fortiadc-d-series/>.

What's new

FortiADC 7.0.1 offers the following new features:

FortiADC-VM support for VMware hardware version 13

FortiADC now supports VMware hardware version 13 which will increase the number of CPUs supported to up to 64 from the previous 8 CPUs. (The maximum number of CPUs supported is limited by the core number of the ESXi server).

OFTP protocol support for FortiAnalyzer logs

FortiADC can now send logs to FortiAnalyzer using the the OFTP protocol which is a private protocol for Fortinet products. Previously, logs can only be sent by syslog protocol — this will continue to be supported alongside the OFTP protocol to ensure continued compatibility with older versions.

Automation enhancements for System and Security Events

System Events and Security Events automations can now be applied to specific virtual servers or real servers.

WAF exceptions support in WAF logs

You can now apply WAF exception rules from WAF logs to reduce false-positives from being logged.

REST API Admin support

You can now create an administrator user account as a REST API Admin user. As a REST API Admin user, you can generate a generalized authorization token to access the FNDN.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, web browsers and Fortinet products supported by FortiADC 7.0.1.

Supported Hardware:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- 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
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)

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

Bug ID	Description
0790383	GUI typo in Security Fabric > Automation: Configuraton → Configuration
0789647	L2 exception list is limited to 300 entries.
0788758	SSL Forward Proxy memory leak.
0783856	CAPTCHA page does not allow <code>Enter</code> key to submit.
0782707/0781234/0775097	Httpoxy-ssl and httpoxy crash related to WAF issues.
0782260	Management interface shows as down.
0782132	Website associated with a VS stops responding intermittently.
0777422	DNS resolving fails for SDN connectors.
0777069	TFTP Health Check script does not work.
0776674	SFP information does not display with <code>diagnose hardware get deviceinfo transceiver</code> CLI command on some hardware models, such as 2200F and 4200F.
0775509	Pop-up window displaying management IP showing in GUI, FortiView > OWASP Top 10 > A1:2017-Injection.
0775262	FortiADC Radius SLB with Dynamic Authorization is not functioning correct and NAT is not applied.
0774824	Action mismatch between WAF alert and Logs.
0774818	GUI typo: Patten → Pattern, Contrain → Constraint
0774178	Application profile does not accept domain names that include numbers.
0773368	High memory and crash due to <code>restapi</code> , <code>httpoxy-ssl</code> and <code>infod</code> .
0772149	FortiADC firewall function failure when the address group name is too long.
0770037	URL that contain "on" in the string (such as "on1" or "one23") is detected as SQL/XSS injection attack.
0766519	NULL pointer dereference in GREP utility.
0766502	Ntpdate crash issue.
0765668	Kernel HA module crash.
0762053	Should implement OFTP support for logging to FortiAnalyzer.
0741343	Disable LLDP on Intel XL710 to solve the flapping issue.

Common Vulnerabilities and Exposures

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

Bug ID	Description
0765175	FortiADC 7.0.1 is no longer vulnerable to the following CVE-Reference: CWE-134: Use of Externally-Controlled Format String.

Known issues

This section lists known issues in version FortiADC7.0.1, but may not be a complete list. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0794045	GUI: For Email automation actions, the From email is sometimes invalidated when it is pasted using <code>Ctrl+v</code> .
0793881	GUI: When selecting multiple entries for automation events, the active selection may become out of sync with the current selection and jump to the top of the menu.
0793861	GUI: The filter function for Status is not working on the Automation page.
0792039	Found the crash event of the REST API (which may be related to the FortiGuard page).
0786198	Two members of the HA cluster reboots unexpectedly at the same time.
0781335	Both AV and IPS currently does not provide any Security Events Alert.
0777188	The GLB cannot connect to the SLB and shows that the licd fails to bind in SLB.
0776212	The traffic triggers A6-CORS protection but the log detail and Dashboard does not display information regarding the A6-CORS protection.
0770641	REST API crash when generating al--in-one debug.
0760557	No warning or log when GLB uses the same port 53 for named and licd.
0730266	Server pool status is misleading.

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 displays the Fortinet Customer Service & Support portal interface. At the top, a blue banner shows a welcome message for Samuel Liu. Below this is a 'Customer Support Bulletin' section with three items listed. The main content area is divided into 'Asset' and 'Assistance' sections. The 'Assistance' section contains links for 'Create a Ticket', 'Manage Tickets', 'View Active Tickets', 'Technical Web Chat', and 'Contact Support'. At the bottom, there are two columns: 'Quick Links' and 'Resources'. In the 'Quick Links' column, the 'Firmware Images' and 'VM Images Download' links are highlighted with a red box. The 'Resources' column lists various support resources like the Customer Support Bulletin, Knowledge Base, and Fortinet Video Library.

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 7.0.1.

Supported upgrade paths

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

Note:

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)

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.

5.1.x to 5.2.x

Direct upgrade via the web GUI or the Console.

5.0.4 to 5.1.x

Direct upgrade via the web GUI or the Console.

Note: allow-ssl-version

There is an old SSL version in the allow-ssl-version config that is not recommend; but the client may have configured it before. This is removed when you upgrade from 5.0.x to 5.1.x/5.2.x. The client may need to add it back manually for compatibility.

5.0.0 to 5.0.4

Direct upgrade via the web GUI or the Console

4.8.x to 5.0.0

Direct upgrade via the web GUI or the Console.

GUI

Due to GUI changes and enhancements, we strongly recommend refreshing (Ctrl +F5) your web browser when access the FortiADC web GUI after the upgrade.

Authentication

This upgrade addresses the compatibility with other devices. Therefore, you must download the new FortiADC SAML SP and upload it to the SAML IDP peer. You do not need to modify the FortiADC SP file anymore.

System

It will take more time to upgrade to 5.0.0 because FortiADC has to create quarantine partition for the AV feature.

GEO IP

You will lose your existing GEO IP protection region configurations when upgrading from 4.7.x to 5.0.0.

4.8.4 to 4.8.4

Direct upgrade via the web GUI or the Console.

4.8.2 to 4.8.3

Direct upgrade via the web GUI or the Console.

4.8.1 to 4.8.2

Direct upgrade via the web GUI or the Console.

4.8.0 to 4.8.1

Direct upgrade via the web GUI or the Console.

GUI

- Due to GUI changes, be sure to refresh your web browser when the upgrade is completed (Ctrl + F5).
- FortiADC 60F supports Google Chrome only.

HA

- To synchronize system image upgrade in HA mode, make sure that all the devices in the HA cluster use exactly the same version of the image.
- Use the management interface in HA mode instead of a dedicated interface.

Platform

- Upgrade your VM01 to 4 GB of memory in virtual platform.

4.7.x to 4.8.0

Direct upgrade via the web GUI or the Console.

- GUI—Due to GUI changes, be sure to refresh (CTRL+F5) your web browser when access FortiADC upon upgrade.
- HA—(For physical devices) Upon upgrade, wait for a few minutes for the HA state to stabilize and the configuration to sync.
- Service—When upgrading to 4.8.x from 4.7.x or lower, FortiADC will add 28 predefined services. If you have old services with the same names as those of the predefined services, FortiADC will rename those "old" services to "oldname_upgrade".
- Global Load Balance—If there was a virtual server pool that was not referenced by any GLB Host in the 4.7.x configuration, the Default Feedback IP configuration in this virtual server pool will be lost upon upgrade. To keep this Default Feedback IP, you MUST reference this virtual server pool in the GLB Host before upgrading the system.

4.6.x to 4.7.x

Direct upgrade via the web UI or the CLI.

- GUI—Due to GUI changes, refresh (CTRL+F5) your web browser when access FortiADC upon upgrade.
- HA—(For physical devices) Upon upgrade, wait for a few minutes for the HA state to stabilize and the configuration to sync.
- Service—When upgrading to 4.7.x from 4.6.x or lower, FortiADC will add 28 predefined services. If you have old services with the same names as those of the predefined services, FortiADC will rename those "old" services to "oldname_upgrade".
- Global Load Balance—If there was a virtual server pool that was not referenced by any GLB Host in 4.7.x configuration, the Default Feedback IP configuration in this virtual server pool will be lost upon upgrade. To keep this Default Feedback IP, you MUST reference this virtual server pool in the GLB Host before upgrading the system.

4.6.1 to 4.6.2

Direct upgrade via the web UI or CLI.

4.5.x to 4.6.x

Direct upgrade to FortiADC 4.6.0 from any version prior to 4.5.x is NOT supported via the GUI. The best way to upgrade is via the CLI using the `restore image` command. If you prefer to upgrade via the GUI, you MUST first upgrade the image to 4.5.x and then to 4.6.x.

- GUI — Due to GUI changes in 4.6.x, be sure to refresh your browser when accessing the new FortiADC web GUI.
- Global Load Balance — If your existing configuration contains the ISP feature, reconfigure it. This is because the ISP option has been moved.
- HA — Update the firmware if HA Sync is enabled. The process normally takes about 10 minutes to complete.

4.4.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.3.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.2.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.1.x to 4.5.x

You can upgrade from FortiADC 4.1.x using the CLI. Direct upgrade from 4.1.x to 4.5.x is not supported from the web UI. See the FortiADC Handbook for instructions on upgrading with the CLI.

4.0.x to 4.5.x

Direct upgrade from 4.0.x and earlier is not supported. You must first upgrade to FortiADC 4.1.x, and the system must be in an operable state.

Upgrading a stand-alone appliance from 4.2.x or later

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.

Settings

System / Settings

Firmware

Partition	Active	Last Upgrade	Firmware Version
1			FA-VMX-4.03.00-FW-build0390-150
2			FA-VMX-4.02.03-FW-build0318-150

Boot Alternate Firmware

Upgrade

HA Sync

☐ Enable

File

Browse...

No file selected.

Select a file to upload.

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 firmware:

1. Go to System > Settings.
2. Click the **Maintenance** tab.
3. Scroll to the Upgrade section.
4. Click **Browse** to locate and select the 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 from 4.3.x or later

The upgrade page for Release 4.3.0 and later includes an option to upgrade the firmware on all nodes in an HA cluster from the primary node.

The following chain of events occurs 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 section.
5. Click **Browse** to locate and select the file.
6. Enable the **HA Sync** option.
7. Click  to upload the firmware and start the upgrade process.
8. Wait for the system to reboot and log you out to complete the upgrade.
9. Clear the cache of your Web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

Note: Normally, it takes approximately up to 10 minutes to upgrade with HA Sync.

Special notes

Suggestions

- HSM doesn't support TLS v1.3. If the HSM certificate is used in VS, the TLS v1.3 handshake will fail.
Workaround: Uncheck the TLSv1.3 in the SSL profile if you're using the HSM certificate to avoid potential handshake failure.
- The backup config file in versions 5.2.0-5.2.4/5.3.0-5.3.1 containing certificate config might not be restored properly (causing config to be lost). After upgrading to version 7.0.1, please discard the old 5.2.x/5.3.x config file and back up the config file in 7.0.1 again.
- Keep the old SSL version predefined config to ensure a smooth upgrade.
- Since the v4.7.x release, FortiADC has introduced a parameter called `config-priority` for HA configuration. It allows you to determine which configuration the system uses when synchronizing the configuration between the HA nodes. Therefore, upon upgrading to FortiADC 4.7.x or higher, we strongly recommend that you use this option to manually set different HA configuration priority values on the HA nodes. Otherwise, you'll have no control over the system's primary-secondary configuration sync behavior.

When the configuration priority values are identical on both nodes (whether by default or by configuration), the system uses the configuration of the appliance with the larger serial number to override that of the appliance with the smaller serial number. When the configuration priority values on the nodes are different, the configuration of the appliance with the lower configuration priority will prevail.

The request-body-detection in the WAF web-attack-signature profile will be changed from "disable" to "enable" automatically after upgrading to FortiADC 5.4.0.

- In version 6.2.0, the default mode of QAT SSL has been changed to polling.
- To use the SRIOV feature, users must deploy a new VM.
- Before downgrading from 7.0.1, 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.
- When deploying the new GSLB based on FortiADC 7.0.0, the verify-CA function will be enabled by default.



FORTINET®



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.