



FortiADC - Release Notes

Version 6.0.4

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/support-and-training/training.html>

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



November 5, 2021

FortiADC 6.0.4 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
Known issues	9
Resolved issues	10
Image checksums	12
Upgrade notes	13

Change Log

Date	Change Description
November 5, 2021	FortiADC 6.0.4 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 6.0.4, Build 0067.

To upgrade to FortiADC 6.0.4, see [FortiADC Upgrade Instructions](#).

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 6.0.4 is a patch release, where no new features and enhancements are covered in this release. See [Known issues on page 9](#) and [Resolved issues on page 10](#) for details.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 6.0.4.

Supported Hardware:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 100F
- FortiADC 200F
- FortiADC 300F
- FortiADC 400F
- FortiADC 1000F
- FortiADC 2000F
- FortiADC 4000F
- 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
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.

Known issues

There are no known issues in FortiADC 6.0.4.

Resolved issues

The following issues have been resolved in FortiADC 6.0.4 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0754366	Abnormal memory usage after upgrade from FortiADC 5.4.4 to 6.0.3.
0752796	A-A VRRP session sync does not work.
0750824	Unexpected reboots of FortiADC device on HA cluster.
0747746	Unable to access GUI and SSH after upgrade from FortiADC 5.3.4 to 6.0.3.
0747637	FortiADC devices fail one after another in HA.
0741029	Unable to establish Windows VPN L2TP through FortiADC.
0740912	Token parse error due to /tmp is full.
0740847	Unable to change password through GUI.
0740226	High CPU and memory utilization caused by dnspod.
0736799	No log name for the SNAT log.
0733833	Constant CPU utilization at 85%+ after importing user defined ISP address.
0731811	Automatic Backups does not work due to special characters in the password.
0728103	Content route matching IP 0.0.0.0 takes precedence which overwrites other content route matching on different IP.
0728077	SNMP retrieves the wrong status for Real Server.
0726621	Real server status showing as "unknown" in GUI.
0725917	FortiGuard Tunneling Username required.
0720273	Interface VLAN returns MAC address as 00:00:00:00:00:00.
0715650	Error on setting secondary IP on loopback interface on Second A-A-VRRP HA node .
0701323	GUI slowness with 255 real servers.
0698484	FortiADC High Availability out of sync. The refcnt cannot be released in netdev_wait_allrefs() because of CLI <code>set dedicate-to-mgmt enable</code> . This leads to dead loop when <code>exec reload</code> .
0687353	Kernel crash due to fib_stat is used after being freed.
0644119	CPU gets stuck due to the fib_cache issue.

Common Vulnerabilities and Exposures

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

Bug ID	Description
0708219	FortiADC 6.0.4 is no longer vulnerable to the following CVE-Reference: CWE-770: Allocation of Resources Without Limits or Throttling

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 present. 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 links 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

Suggestions

- 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 6.0.4, please discard the old 5.2.x/5.3.x config file and back up the config file in 6.0.4 again.
- Keep the old SSL version predefined config to ensure a smooth upgrade.
- HSM does not support TLSv1.3. If the HSM certificate is used in VS, the TLSv1.3 handshake will fail.
Workaround: Uncheck the TLSv1.3 in the SSL profile if you are using the HSM certificate to avoid potential handshake failure.



FORTINET®



Copyright© 2021 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.