



FortiADC - Release Notes

Version 5.3.7



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://fortiguard.com/

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



December 8, 2020 FortiADC 5.3.7 Release Notes 01-537-683708-20201208

TABLE OF CONTENTS

Change Log	4
Introduction	
What's new	6
Hardware and VM support	7
Known issues	
Resolved issues	9
Image checksums	10
Upgrade notes	11

Change Log

Date	Change Description
2020-12-08	FortiADC 5.3.7 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 5.3.7, Build 0680.

To upgrade to FortiADC 5.3.7, 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 5.3.7 addresses issues concerning high CPU/memory usage caused by the infod process, as well as other bug fixes. There are no new features.

Hardware and VM support

FortiADC 5.3.7 supports the following hardware models:

- 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 Release 5.3.7 supports deployment of FortiADC-VM in the following virtual machine environments:

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
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

Known issues

There are no known issues discovered in FortiADC 5.3.7 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

The following issues have been resolved in FortiADC 5.3.7 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

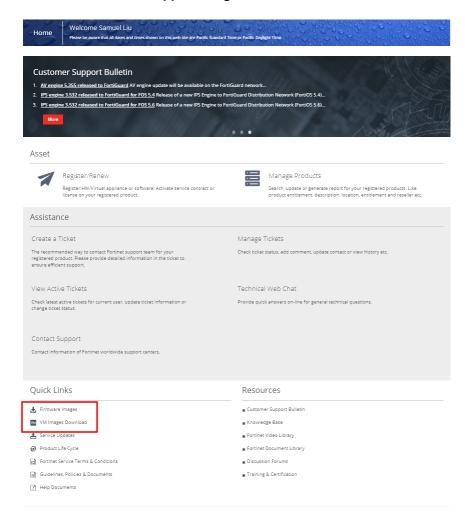
Bug ID	Description
670196	CPU /memory high caused by infod
672916	SSL server closed the connection but FortiADC did not close any side of the connections
673592	GLB stopped completely due to invalid zone txt record
670149	One virtual server stopped working

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

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 5.3.7, please discard the old 5.2.x/5.3.x config file and back up the config file in 5.3.7 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.





Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGate®, 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.