FortiADC - Release Notes

Version 5.4.3

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

July 17, 2020
FortiADC 5.4.3 Release Notes
01-543-651415-20200717

TABLE OF CONTENTS

Change Log 4
Introduction 5
What's new 6
Hardware and VM support 7
Known issues 8
Resolved issues 9
Image checksums 10
Upgrade notes 11

Change Log

Date	Change Description
2020-07-17	FortiADC 5.4.3 Release Notes initial release.
2020-07-30	Added bug 653209 to Known Issues

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 5.4.3, Build 0737.

To upgrade to FortiADC 5.4.3, see FortiADC Upgrade Instructions.

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 5.4.3 offers the following new features:

- signature profiles support limitation of body scanning

Hardware and VM support

FortiADC 5.4.3 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 5000F

FortiADC Release 5.4.3 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

This section highlights the major known issues discovered in FortiADC5.4.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Known issues

Bug ID	Description
653209	If your password includes any of the following special characters: backslash (\), single quote ('), or double quote (''), you may get an incorrect password error when entering in your password. **Workaround:** When entering in your password, add a backslash (\) before each of the special characters and enclose the entire password in double quotes. For example, if your password is 1\2"3'4, you should type "1\\2\"3\'4" during authentication. This issue is scheduled to be fixed in the next release.

Resolved issues

The following issues have been resolved in FortiADC 5.4.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

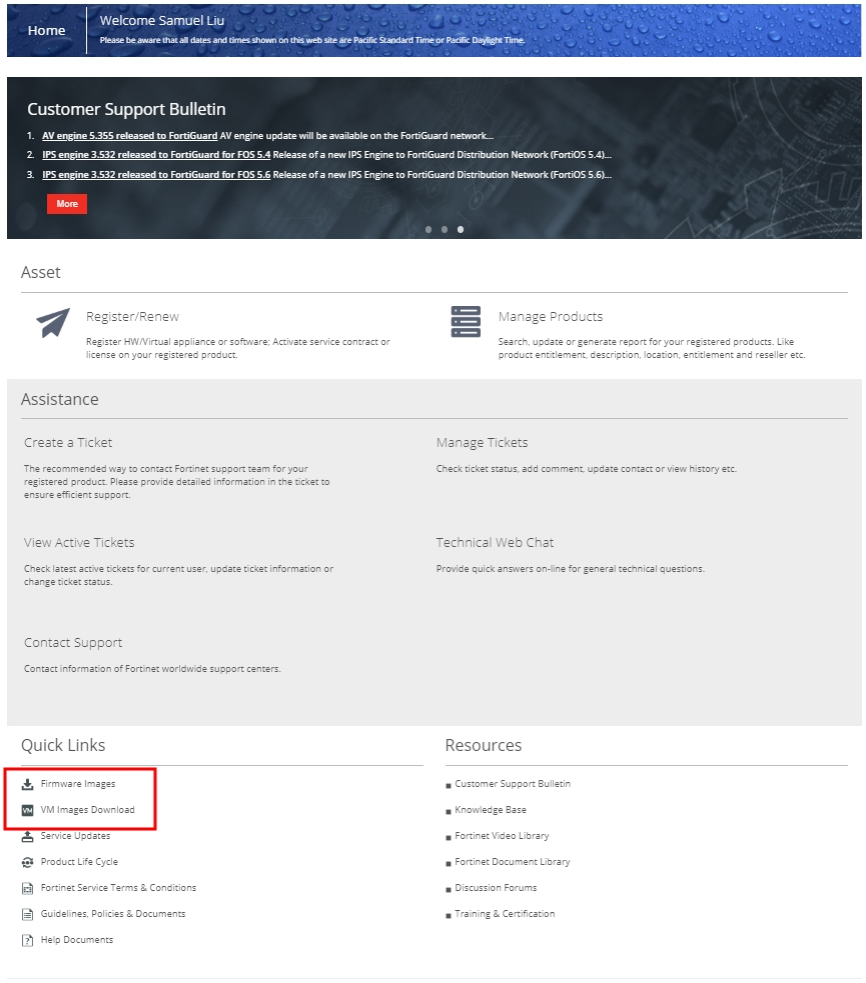
Bug ID	Description
640543	SNAT wrongly NATed after LLB failover
646954	The Diag commands do not decrypt TLS1.3
608575	MYSQL application profile not allowing connection to master or slave
644221	Shutdown of Hyper-V instance fails
641421	httproxy-ssl crash
643217	GUI Not Accessible
638621	L7VS will not process traffic when error page and RS pool share the same name
638415	HA AP slave node with dedicated management should use master node as FDS proxy
641772	OWA Logoff does not work when custom authentication form is used
640737	Ips related items missed in fast report
635876	Fortiview-slb-data analytics should not show quarantine monitor
649474	Error page does not work
637188	CLI crashes when checking auto update versions.
636429	Should not show warning when zone TXT record name is same as domain name
649323	SLB SIP traffic log shows the real server's IP instead of real server's name when use source address hash persist
648667	Some ISO8583 profile's content should not be displayed for other type profile

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 5.4.3, please discard the old V5.2.x/V5.3.x config file, backup the config file in V5.4.3 again.
- Keep the old SSL version predefined config to ensure a smooth upgrade.
- HSM does not support TLVv1.3. 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®, 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.