FortiADC - Release Notes

Version 5.3.3

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

October 24, 2019
FortiADC 5.3.3 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-10-23	FortiADC 5.3.3 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.3.3, Build 0655.

To upgrade to FortiADC 5.3.3, 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 5.3.3 offers the following new features:

Global Server Load Balance

DNS Certification Authority Authorization (CAA) is an Internet security policy mechanism which allows domain name holders to indicate to certificate authorities whether they are authorized to issue digital certificates for a particular domain name. It does this by means of a new "CAA" Domain Name System (DNS) resource record.

Hardware and VM support

FortiADC 5.3.3 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 Release 5.3.3 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

There are no known issues discovered in FortiADC 5.3.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

This section highlights the major known issues discovered in FortiADC 5.3.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Known issues

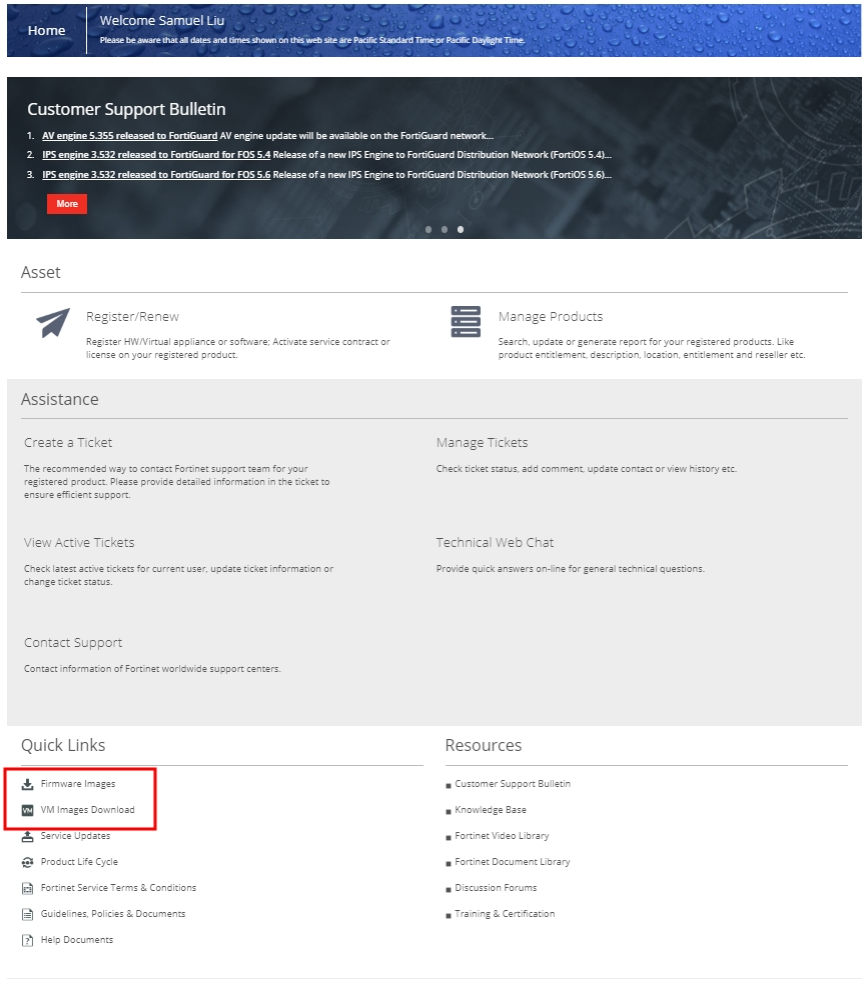
Bug ID	Description
0589864	The DDoS number on the dashboard may keep increasing in particular circumstances.
0587743	The DDoS of L7-HTTP-VS may cause crashes in some circumstances due to the memory being overwritten.
0583205	Authentication cookie timeout for L7-HTTP/HTTPS VS is not configurable
0589136	L7-VS scripting may add additional $ sign before a cookie key string.
0588896	Cookie security cannot work together with hidden field, CSRF.
0586257	L4-VS NAT46 mode may not work in some circumstances.
0588652	WAF CSRF: incorrect cookie handling causes the user to be unable to log into the DVWA portal.
0585307	Some FortiView statistics field may have no data if the L4-VS is with port-range configs
0588247	WAF report may not show the attacks of CSD in some circumstances.
0534061	Changing the DNS server config may cause L7-HTTPS VS to use the old DNS settings to do the OCSP and CRLDP, until you disable then enable the VS.
0583761	The VM license may be authenticated by the FortiGuard service due to the domain "update.fortiguard.net". In these cases, it may be also flushed away in particular circumstances.
0581492	Hide the clone button for WAF alert to avoid mislead the customer.
0585209	DNS Certification Authority Authorization (CAA) Resource Record supported by GLB server.
0503199	Factoryreset cannot delete hsm certificates.
0585853	There could be memory leak happening on flg_reportd daemon in particular circumstances.
0584723	Some particular DDoS config may cause kernel panic.
0584504	The health-check module may stop working suddenly with a lot of health-check scripts.
0584216	There could occur core crash happening on 4000F in some circumstances.
0583416	The configuration of the HSM server should be cleared if you click "unregister."
0503346	[HSM] If the partition exists, the unregister is not allowed.
0590433	There should be protections for the WAF function to avoid a L7-VS crash.

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

The backup config file in V5.2.0-5.2.4/V5.3.0-V5.3.1, which contains certificate config may not be restored properly (causing config lost). After upgrading to V5.3.2, please discard the old V5.2.x/V5.3.x config file, then backup the config file in V5.3.2 again. This should solve the problem.

Keep the old SSl version

Keep the old SSL version predefined config to allow the upgrade to continue smoothly.

TLSv1.3 handshake failure

HSM doesn't support TLVv1.3. If the HSM certificate is used in VS, the TLSv1.3 handshake will fail.

Workaround: Please uncheck the TLSv1.3 in the SSL profile if you are using the HSM certificate to avoid potential handshake failure.

Adjust boot partition

To upgrade image for VM platfroms, because of the boot partition size limit before 5.1.x, please be sure to upgrade to 5.1.x image first to adjust boot partition size, then upgrade to 5.2.x and 5.3.x, or else it will report "Unmatched partition size" error when upgrading.

No such issue for physical platforms.