FortiADC - Release Notes

Version 5.3.6

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

August 31, 2020
FortiADC 5.3.6 Release Notes
01-536-660861-20200831

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-08-27	FortiADC 5.3.6 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 5.3.6, Build 0679.

To upgrade to FortiADC 5.3.6, 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 5.3.6 offers the following new features:

Shared Resources

Health Checks

The default down retry value has been changed from 1 attempt to 3 attempts, allowing for more tries before determining the server status to be down.

The default interval time has been changed from 10 seconds to 5 seconds, and the default timeout has been changed from 5 seconds to 3 seconds.

Hardware and VM support

FortiADC 5.3.6 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 5.3.6 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 5.3.6 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

The following issues have been resolved in FortiADC 5.3.6 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

Bug ID	Description
644119	CPU gets stuck and device becomes inoperative
620616	ADC CPU at 100% usage and stops responding
616646	Fetch DN issue when there are multiple spaces
625266	Request old password before allowing user to change password
644221	Shutdown of Hyper-V instance fails
643217	GUI not accessible
616628	MIB Misspelling on facdTrapSysCrlExpires
638621	L7VS will not process traffic if error page and RS pool share the same name
618398	Route Health Injection (RHI) for OSPF and BGP are not working with non-root vdom
619764	Connections to msgctrl1.fortinet.com do not use FortiGuard tunnel
641421	Httproxy-ssl crashes
614083	Forward Proxy doesn't add the certificate chain along with the signed cert during TLS handshake.
627651	Connection reset by L7 SMTP VS
633350	LACP interface intermittently down
650760	Software switch interface displayed on the HA remote IP monitor if it is accessed to FGT through GUI.
620051	Source NAT pool setting does not work well.
640543	SNAT wrongly NATed after LLB failover
628261	L2 Load Balancing configured along with Content Routing rules cause break to Content Routing
651561	netlink interface list portX linkstat unrealistic counters output
652382	Remote IP Monitor List not shown on the GUI in HA settings when language is Japanese
594801	Resource Usage and Server Load Balance graph has no data
609969	Synchronization status stuck at Not sync due to the special characters in admin password settings.

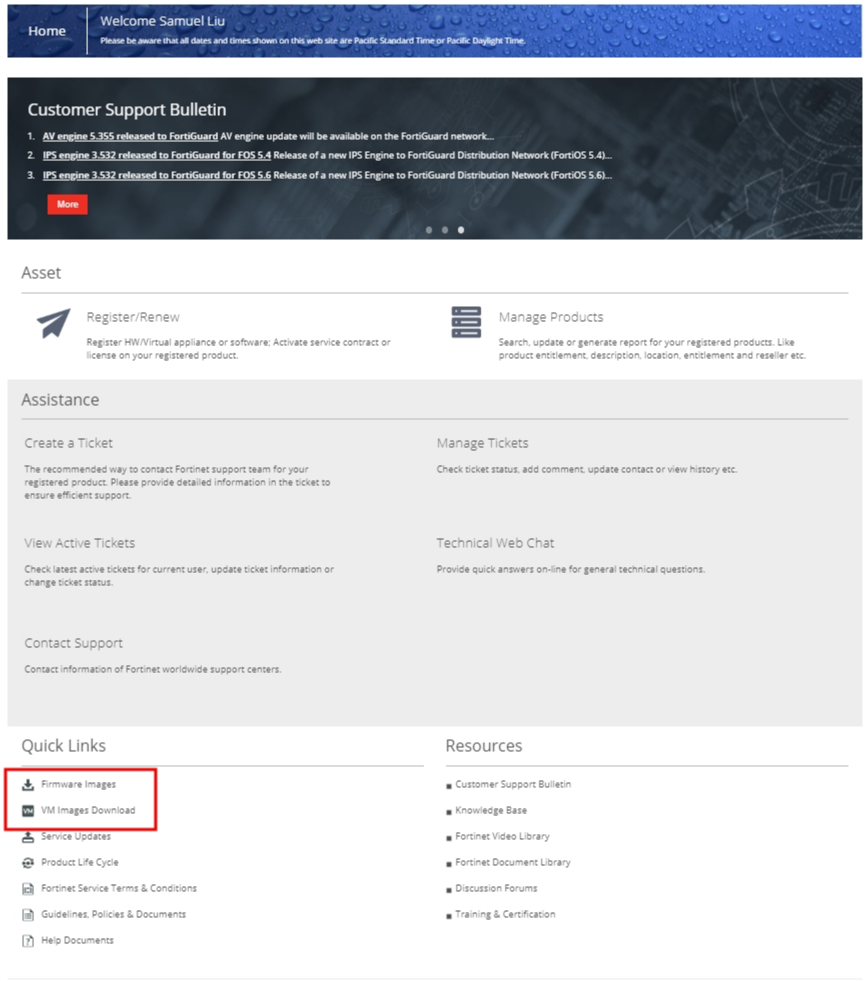
Bug ID	Description
614682	Losing Internet access and the access of websites published via VRRP Active-Active ADC sporadically.
623196	Changes via GUI for HA only not occurring
611170	IP address conflict Event Logs observed in Master node of HA-AA
607420	Non working VRRP ADC node generates Router LSA for the active ippool addresses causing services to fail.
638415	HA AP slave node with dedicated management should use master node as FDS proxy
626517	Generic error message with admin user configuration
625035	Add a CLI for 40G interface promiscuous mode
612763	httproxy crashes when ddos http and AV are enabled
611334	WAF OWASP TOP10 load failed, load info db failed
625195	Plenty of update result system event log after deploy ADC
614963	Incorrect connections is shown on Dashboard SLB when waf_heur_sqlxss_inject_detect appears
632894	VS status changing causes some packets drop
617299	FAD VM shutdown incomplete on vmware
633570	SNAT doesn't work for the existing session after reboot in some circumstances
631916	SLB ISO8583 has transactions with null response when response is received in different orders as sending
631943	LLB gw status is not correct after changing gw ip to subnet that is not directly connected to ADC
622287	All-in-one debug enhancement to collect more information
623635	cookie security stability enhancement
634774	Adjust the default value for the health check parameters
658496	LLB nexthop gateway remain unchanged despite updated configuration
616356	SSL - Server Accepts Weak Diffie-Hellman Keys SSH - Weak MAC Algorithms

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



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 FOS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FOS 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 5.3.6, please discard the old 5.2.x/5.3.x config file and back up the config file in 5.3.6 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.

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.