FortiADC - Release Notes

Version 5.4.5

April 6, 2021
FortiADC 5.4.5 Release Notes
01-541-607360-20200214

TABLE OF CONTENTS

Change Log

Date	Change Description
April 6, 2021	FortiADC 5.4.5 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 5.4.5, Build 0754.

To upgrade to FortiADC 5.4.5, 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 5.4.5 is a patch release only; no new feature or enhancement has been implemented in this release.

Hardware and VM support

FortiADC 5.4.5 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 5.4.5 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

FortiADC 5.4.5 does not have known issues. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

The following issues have been resolved in FortiADC 5.4.5 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Resolved issues

Bug ID	Description
0708068	Intermittency issues happen after upgrade to 6.1.1, which are caused by IPv6 route.
0699499	FortiADC does not answer DNS query sent with Dig when the CNAME type flag is missing.
0698833	Add option for customer to enable/disable TCP timestamp response.
0692841	Some Real Server pools don't show up the members in GUI, which is caused by restapi crash.
0682988	All logs stops working and CPU utilization is increased.
0682666	Admin user with Read-only access can still change network interface settings.
0679167	FortiADC is unable to save configuration due to oldschool ssh library.
0678787	LDAP config doesn't work.
0677102	FortiADC Manager disconnects from FortiADC periodically.
0676693	HA Active-Passive: any change results in Not in Sync.
0676126	Memory start to increase after a while.
0673408	High memory usage after upgrade from 5.3.5 to 5.3.6.
0670544	Enlarge L2 exception list member to 1K.
0700969	[Azure] Cannot manage FortiADC after boot through SSL when using PAT.
0694749	Virtual tunnel stops to work.
0694518	Crtl+c when the vdom is being deleted will cause CLI to crash.
0693312	The RADIUS attribute persistency does not work properly.
0692276	Unable to change password in GLB setting auth if input values and change auth method.
0690616	The authd may crash if multiple session uses the same user to login.
0689295	GUI slows with 255 real servers.

Bug ID	Description
0688374	SAML authentication - Internal Server Error.
0688036	Memory leak caused by licd.
0685273	Aggregate interface is still up when connected switch bond is disabled.
0682890	Run the sync-list from GUI is failed due to password is missing in the HTTP get parameter.
0676775	GLB connection-limit does not work after disable/enable GLB.
0674992	Modify master to primary for FortiADC warning when HA mode.
0670196	CPU /memory high caused by infod.
0463003	Interface light state is wrong on 200D/2KF/4KF.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

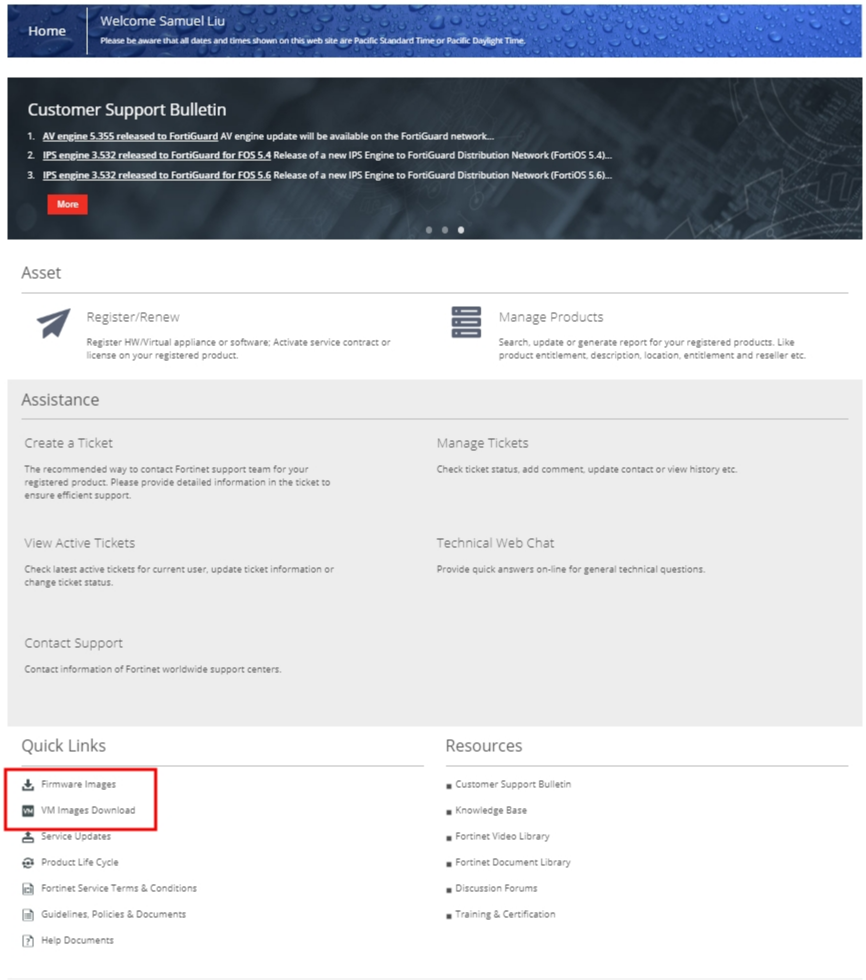
684277	FortiADC5.4.5 is no longer vulnerable to the following CVE-Reference: CVE-2019-6693.
684276	FortiADC 5.4.5 is no longer vulnerable to the following CVE-Reference: CVE-2018-13374.
684275	FortiADC 5.4.5 is no longer vulnerable to the following CWE-Reference: CWE-749.

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

The request-body-detection in the WAF web-attack-signature profile will be changed from "disable" to "enable" automatically after upgrading to FortiADC5.4.5.