FortiADC Release Notes

Version 5.1.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

Monday, July 1, 2019

FortiADC 5.1.6 Release Notes

First Edition

TABLE OF CONTENTS

Change Log

Date	Change Description
7/1/2019	FortiADC 5.1.6 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.1.6, Build 0268.

To upgrade to FortiADC 5.1.6, 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

There are no new features for the FortiADC 5.1.6 release.

Upgrade notes

allow-ssl-version

There is an old SSL version in the allow-ssl-version config that is not recommend; but the client may have configured it before. This is removed when you upgrade from 5.0.x to 5.1.x/5.2.x. The client may need to add it back manually for compatibility.

Hardware and VM support

FortiADC 5.1.6 supports the following hardware models:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 60F (without HSM, PageSpeed, and AV features)
- FortiADC 100F
- FortiADC 200F
- FortiADC 1000F
- FortiADC 2000F
- FortiADC 4000F

FortiADC Release 5.1.6 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
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

Resolved issues

This section lists the major known issues that have been resolved in this 5.1.6 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
0560607	Geoip db update may cause coredump and link down
0558190	NAT Pool Traffic Status
0558956	Unable to change the ahead time/interval on OCSP Stapling.
0560927	OU are increased depending on number of space when generate local certificate thru GUI.
0557564	ADC cannot forward icmp (type 0, code 4) to RS on L4VS mode.
0561679	When saml-sp and idp use a long name the shibd ps does not start
0561466	AWS，move floating IP fail when HA fail over
0554666	Traffic Not Being Sent To Real Servers
0555267	L4 traffic is reconnected and stops if RS is set to "maintain" in Real Server
0549676	Unable To Deploy HyperV VM
0549816	[Hyper-V] should support deploying ADC by import template on windows server 2019
0551354	Lost ip address when changing the Interface mode from dhcp to static
0550399	lb routing in script does not work when a content-routing name contains another
0556482	Restrictions for Creating Admin User Accounts
0555919	File Security: HTTPproxy Memory leak
0555060	RTT and APP response in RS reversed on Fortiview
0554604	Using HTML form on 'Client Authentication Method' removes character from LDAP username.
0553019	Health check limit to 128

Bug ID	Description
0552901	Sync List Not Working
0552636	ADC vulnerable to CVE-2017-17544 & CVE-2018-13366
0538163	Admin User Authenticated by LDAP Cannot Change the ‘Global Admin’ Value
0551144	GSLB incorrect backup state propagation on FortiView
0553378	OCI, After uploading privilege.key, can not deploy in configuration.
0553011	After selecting local cert and issuer cert, when saving, ADC should check if the local cert is issued by the issuer cert; if not, it should return error message.

Known issues

There are no known issues discovered up to the FortiADC 5.1.6 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

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.

Figure 1: Customer Service & Support image checksum tool