

# FortiADC Release Notes

**Version 5.1.5**

**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](mailto:techdocs@fortinet.com)



Thursday, April 25, 2019

FortiADC 5.1.5 Release Notes

First Edition

# TABLE OF CONTENTS



<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>What's new</b> .....	<b>6</b>
<b>Upgrade notes</b> .....	<b>7</b>
<b>Hardware and VM support</b> .....	<b>8</b>
<b>Resolved issues</b> .....	<b>9</b>
<b>Known issues</b> .....	<b>10</b>
<b>Image checksums</b> .....	<b>14</b>

## Change Log

Date	Change Description
4/25/2019	FortiADC 5.1.5 Release Notes initial release.

# Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.1.5, Build 0266.

To upgrade to FortiADC 5.1.5, 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 5.1.5 offers the following new feature:

### **Additional “response-half-closed-request” option to HTTP/HTTPS/TCP/SSL/RDP load-balance profile**

This option will allow the FortiADC to serve the request and send back the response even if the client closes the output channel.

In some cases, the client may close the output channel even after sending out the request; but at the same time the client will be waiting for a response. If this option is disabled, the FortiADC will abort, and will not serve the request anymore once it receives notice that the client has closed the channel. This may cause clients to complain of failures.

# 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 5.1.5 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 5.1.5 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
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 5.1.5 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

**Table 1: Resolved issues**

Bug ID	Description
0526487	Mobile email not refreshing
0549539	The local certificate cannot be uploaded when the entries count are equal to 93.
0552895	httproxy crash for FAD_AP_SSL_Empty_Reply with traffic
0539896	After upgrading from 4.8.6 to 5.1.3 - and after deleting HTTP L7VS- get duplicate L7VS entries and add it back
0552401	RSP RS status is not right and traffic still goes to nonexistent RS in session.
0549758	If the TTL of packet is 1, there could be an alert for IP Pool Exhaust.
0550194	Importing san-certificate for management makes https go down.
0545652	LLB tunnel source destination hash is dropping packets on 60F
0548490	L7VS is forwarding traffic to a server that is disabled when persistence is CHASH
0546251	Switch ports on the FortiADC loses member ports
0544663	AV coredump happened during waf-csrf testing

## Known issues

This section highlights the major known issues discovered up to the FortiADC 5.1.5 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

**Table 2: Known issues**

Bug ID	Description
0468417	<p>Changes made to the destination port of the VXLAN tunnel do not take effect on the listening port.</p> <p><b>Workaround:</b> Normally, you do not need to change the destination port. If you do, be sure to reboot the system.</p>
0465516	<p>The order of the Interfaces could get changed after removing and re-adding an interface to FortiADC in an OpenStack environment.</p> <p><b>Workaround:</b> Determine the number of interfaces before configuration, and try not to delete interfaces in an OpenStack environment.</p>
0470620	<p>OpenStack Ibass cannot connect to backup FortiADC devices after a failover.</p> <p><b>Workaround:</b> Manually configure the device settings when FortiADC is in HA-AA or HA AA-VRRP mode.</p>
0471518	<p>For Layer-2 and Layer-4 TCP or TCPS profiles, and Layer-7 Turbo HTTP profile, the FortiView&gt;Server Load Balance&gt;Virtual Server page can display Throughput, Concurrent Connections, and Health Status of virtual servers or real servers.</p>
0471525	<p>If <code>client-certificate-verify-option</code> in a <code>client_SSL_profile</code> is set to "Optional", the persistence type <code>LB_PERSIS_SSL_SESS_ID</code> will not work in a virtual server which uses the <code>client_SSL_profile</code>.</p> <p><b>Workaround:</b> Do NOT set <code>client-certificate-verify-option</code> in a <code>client_SSL_profile</code> to "Optional".</p>
0401984	<p>The IP table rules created by <code>rtsp_vs</code> could not sync to the slave device in HA mode.</p> <p><b>Workaround:</b> You must re-connect to the RTSP server when performing HA sync.</p>
0233369	<p>Shutting down the PPPoE interface sometimes could cause the default route to be deleted from the default route table.</p> <p><b>Workaround:</b> Reconfigure the default route table after shutting down the PPPoE interface.</p>

Bug ID	Description
0380628	<p>Sometimes, global load-balance link member configuration in HA VRRP configuration could not be fully synced to the slave device.</p> <p><b>Workaround:</b> When that happens, execute the command "<code>execute ha force sync-config</code>" to sync the configuration.</p>
0401508	<p>When FortiADC is in an HA active-passive configuration using a switch in transparent mode with the STP function enabled, traffic could get interrupted briefly when a fail-over occurs.</p> <p><b>Workaround:</b> The interruption occurs because STP needs time to re-learn in order to adjust. This is not a FortiADC issue. You can change STP configuration in the switch to prevent this from happening.</p>
0376784	<p>Some traffic log data may go missing when FortiADC is under heavy traffic stress.</p> <p><b>Workaround:</b> Enable traffic logging only in normal traffic conditions; do NOT enable it when CPU usage exceeds 60%.</p>
0372459	<p>Sometimes, the floating IP may be missing in the back-end after some operations.</p> <p><b>Workaround:</b> When that happens, reconfigure the floating IP.</p>
0414143	<p>The traffic limit control for FortiADC inbound/outbound packets in each VDOM only works for TCP traffic; it does not work for UDP traffic.</p> <p><b>Workaround:</b> Do NOT impose the traffic limit on UDP traffic.</p>
0377176	<p>The OSPF neighbor won't be built if the floating IP is the same as the interface IP.</p> <p><b>Workaround:</b> Avoid setting the floating IP the same as the interface IP.</p>
0446943	<p>SSL throughput may decrease under certain circumstances.</p> <p><b>Workaround:</b> Tune the <code>tune-bufsize</code> to 16384.</p>
0444752	<p>When 300 wildcard administrators using different RADIUS servers in the system, it may take up to 5 minutes to log in.</p> <p><b>Workaround:</b> Try to use no more than 10 RADIUS/LDAP servers for wildcard administrator authentication.</p>
0448922	<p>Some VDOM configurations may remain in the system if you delete a VDOM shortly after it is created.</p> <p><b>Workaround:</b> Do not create and delete VDOMS in a rapid fashion.</p>

Bug ID	Description
0481306	<p>On the Oracle OCI compute instance management page, rebooting an instance may take more than 10 minutes.</p> <p><b>Workaround:</b> This is OCI-specific issue. Reboot Oracle OCI instances from FortiADC GUI or Console instead.</p>
0499140	<p>Sometimes, the <b>Web Application Firewall&gt; Web Attack Signature&gt; Signature</b> page does not show detailed information.</p> <p><b>Workaround:</b> Refresh page, or switch to another page and then switch back.</p>
0495277	<p>After a file is submitted to FortiSandbox, it may take a while for the AV module to generate the "File submitted to Sandbox" log.</p>
0488973	<p>"diagnose antivirus database-info" shows version in format like 05/03/0018 instead of 05/03/2018.</p>
0499175	<p>The Web Vulnerability Scanner task page cannot refresh automatically.</p> <p><b>Workaround:</b> Once a new task has started, click the Refresh button to get latest task status.</p>
523216	<p>If the backup configuration is saved by admin user whose name includes '_' before 5.1.2, it will not be listed after upgrading to 5.2.0</p> <p><b>Workaround:</b> Before upgrading to 5.2.0, redo backup by another admin user whose name does not include '_'</p>
515275	<p>Global Load Balance supports new "server-performance" method in virtual server pool, but for the remote servers which are running an image before 5.2.0, it will not report performance information to GLB server, so it will be treated as the worst performance server in the pool.</p>
526074	<p>In slave device of HA AP mode, ping HA mgmt ip of itself may fail</p>
518447	<p>On Google Cloud Platform(GCP) VM does not support the following features:</p>
518448	<ul style="list-style-type: none"> <li>• HA AP mode</li> </ul>
518446	<ul style="list-style-type: none"> <li>• HA AA mode</li> </ul>
518449	<ul style="list-style-type: none"> <li>• Floating IP of interface</li> </ul>
517138	<ul style="list-style-type: none"> <li>• IPv6</li> <li>• VLAN interface</li> <li>• Softswitch interface</li> <li>• Aggregate interface</li> </ul>

Bug ID	Description
530020	On Azure the VM does not support the following features: <ul style="list-style-type: none"> <li>• HA AP mode</li> <li>• HA AA mode</li> <li>• VLAN interface</li> <li>• Softswitch interface</li> <li>• Aggregate interface</li> </ul>
530017	On AWS the VM does not support the following features: <ul style="list-style-type: none"> <li>• HA AP mode</li> <li>• HA AA mode</li> <li>• VLAN interface</li> <li>• Softswitch interface</li> <li>• Aggregate interface</li> </ul>
524335	SIP sessions CPS performance drops when source address is enabled
518048	In FortiGuard Services, please be reminded that the system will reload and traffic may be interrupted after you upgrade/reset "Geo IP"
528695	In Cloud platform(AWS/GCP/Azure/Aliyun), after changing the IP settings in ADC, like VS IP, or interface ip/secondary ip etc, please also change the IP configuration of the interface in cloud networking
514583	GUI>Global>System File, -- it only supports uploading a file up to 300M.
542995	HSM only supports V5.

# 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.

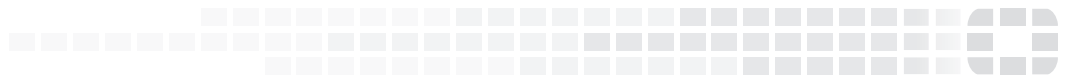
MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support 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**

The screenshot displays the Fortinet Customer Service & Support website interface. At the top, there is a navigation bar with a 'Home' link and a welcome message for 'Samuel Liu'. Below this is a 'Customer Support Bulletin' section with three items related to AV and IPS engine updates. The main content area is divided into several sections: 'Asset' (with 'Register/Renew' and 'Manage Products' options), 'Assistance' (with 'Create a Ticket', 'View Active Tickets', 'Contact Support', 'Manage Tickets', and 'Technical Web Chat' options), 'Quick Links', and 'Resources'. In the 'Quick Links' section, the 'Firmware Images' and 'VM Images Download' links are highlighted with a red box. The 'Resources' section includes links to 'Customer Support Bulletin', 'Knowledge Base', 'Fortinet Video Library', 'Fortinet Document Library', 'Discussion Forums', and 'Training & Certification'.



High Performance Network Security



Copyright© 2019 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.