


# FortiADC Release Notes

**Version 5.0.4**

**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

Thursday, August 9, 2018

FortiADC 5.0.4 Release Notes

First Edition

# TABLE OF CONTENTS


**Change Log** ..... **4**
**Introduction** ..... **5**
**What's new** ..... **6**
**Special note** ..... **7**
**Hardware and VM support** ..... **8**
**Resolved issues** ..... **9**
**Known issues** ..... **10**
**Image checksums** ..... **13**

# Change Log

| Date | Change Description |
| --- | --- |
| 08/10/2018 | FortiADC 5.0.4 Release Notes initial release. |

# Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.0.4, Build 0072.

To upgrade to FortiADC 5.0.4, 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 5.0.4 is a patch release only; no new feature or enhancement has been implemented in this release.

# Special note

To further enhance system performance, this release sees the removal of two legacy interfaces from the Hyper-V platform. The newly deployed Hyper-V platform has only eight (8) interfaces.

# Hardware and VM support

FortiADC 5.0.4 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 5.0.4 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 5.0.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

**Table 1: Resolved issues**

| Bug ID | Description |
|---|---|
| 0502349 | FortiADC VMs might be unable to restore configuration files via TFTP if the license is loaded right after boot-up. |
| 0504249 | IPv6 unique local addresses may not work properly. |
| 0503051 | FortiADC lacks a SNMP trap configuration for TRAP_TYPE_PSU_Failure. |
| 0503965 | The VM license file needs to be uploaded after it's become pending. |
| 0504457 | Unstable internet access could cause license status to become pending and prompt the user to upload a new license. |
| 0503066 | FortiADC may send a RADIUS ACCESS REQUEST packet on RADIUS accounting port. |
| 0478703 | The VLAN interface in an HA VRRP configuration could not be reached. |
| 0506522 | A Layer-7 virtual server using the SMTP protocol could disrupt the connection between a client (FortiMail) and a real server (Exchange) under certain circumstances. |
| 0505726 | Memory usage could spike up for a single httproxy process and stay high even during non-working hours. |
| 0506745 | An SMTP virtual server could stop working after some configurations changes were made. |
| 0506615 | HA priority configuration changes may cause kernel crash. |
| 0480655 | Log download could fail due to system timeout when a large number of logs were involved. |

# Known issues

This section highlights the major known issues discovered in FortiADC 5.0.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

**Table 2: Known issues**

| Bug ID | Description |
|---|---|
| 0412861 | The aggregate interface can not work under balance-rr/xor/broadcast with the switch in HA mode.<br>**Workaround:** Traffic return from peer switch may go to slave node. Use another algorithm instead. |
| 0455272 | GEO IP configurations would get lost when restoring a pre-5.0 version from v5.0.<br>**Workaround:** Do not restore the configuration of a lower version on a v5.0 system directly. |
| 0468417 | Changes made to the destination port of the VXLAN tunnel do not take effect on listening port.<br>**Workaround:** Normally, you do not need to change the destination port. If you do, be sure to reboot the system. |
| 0465516 | The order of the Interfaces could get changed after removing and re-adding an interface to FortiADC in an OpenStack environment.<br>**Workaround:** Determine the number of interfaces before configuration, and try not to delete interfaces in an OpenStack environment. |
| 0470620 | OpenStack lbass cannot connect to backup FortiADC devices after a failover<br>**Workaround:** Manually configure the device settings when FortiADC is in HA-AA or HA AA-VRRP mode. |
| 0471518 | For Layer-2 and Layer-4 TCP or TCPS porfiles, and Layer-7 Turbo HTTP profile, the FortiView>Server Load Balance>Virtual Server page can display Throughput, Concurrent Connections, and Health Status of virtual servers or real servers. |
| 0471525 | If `client-certificate-verify-option` in a client_SSL_profile is set to "Optional", the persistence type LB_PERSIS_SSL_SESS_ID will not work in a virtual server which uses the client_SSL_profile.<br>**Workaround:** Do NOT set `client-certificate-verify-option` in a client_SSL_profile to "Optional". |

| Bug ID | Description |
|---|---|
| 0475733 | Script content was lost when downgrading from 5.0.0 to 4.8.4.<br>**Workaround:** Downgrading from 5.0.0 to lower versions is not supported. Be sure to back up your configuration before upgrading to 5.0.0. |
| 0401984 | The IP table rules created by rtsp_vs could not sync to the slave device in HA mode.<br>**Workaround:** You must re-connect to the RTSP server when performing HA sync. |
| 0233369 | Shutting down the PPPoE interface sometimes could cause the default route to be deleted from the default route table.<br>**Workaround:** Reconfigure the default route table after shutting down the PPPoE interface. |
| 0380628 | Sometimes, global load-balance link member configuration in HA VRRP configuration could not be fully synced to the slave device.<br>**Workaround:** When that happens, execute the command "`execute ha force sync-config`" to sync the configuration. |
| 0401508 | 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.<br>**Workaround:** 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. |
| 0376784 | Some traffic log data may get missing when FortiADC is under heavy traffic stress.<br>**Workaround:** Enable traffic logging only in normal traffic conditions; do NOT enable it when CPU usage exceeds 60%. |
| 0372459 | Sometimes, the floating IP may be missing in the back-end after some operations.<br>**Workaround:** When that happens, reconfigure the floating IP. |
| 0414143 | The traffic limit control for FortiADC inbound/outbound packets in each VDOM only works for TCP traffic; it does not work for UDP traffic.<br>**Workaround:** Do NOT impose the traffic limit on UDP traffic. |
| 0377176 | The OSPF neighbor won't be built if the floating IP is the same as the interface IP.<br>**Workaround:** Avoid setting the floating IP the same as the interface IP. |
| 0446943 | SSL throughput may decrease under certain circumstances.<br>**Workaround:** Tune the tune-bufsize to 16384. |

| Bug ID | Description |
|---|---|
| 0444752 | When 300 wildcard administrators using different RADIUS servers in the system, it may take up to 5 minutes to log in.<br>**Workaround:** Try to use no more than 10 RADIUS/LDAP servers for wildcard administrator authentication. |
| 0446418 | After migrating RADIUS persistence profiles to Version 4.8.1, some vendor-specific attributes may get lost during backup and restore.<br>**Workaround:** Vendor-specific attributes with empty values are for backward compatibility, and not intended for RADIUS persistence. You need to modify the configuration in 4.8.1. |
| 0448922 | Some VDOM configurations may remain in the system if you delete a VDOM shortly after it is created.<br>**Workaround:** Do not create and delete VDOMS in a rapid fashion. |

# 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**