High Performance Network Security

FortiADC D-Series Release Notes

Release 4.5.2

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

FORTINET®

Tuesday, July 19, 2016

FortiADC D-Series Release Notes 4.5.2

Revision 1

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-07-19	Initial release.

Introduction

This document provides a list of new features and enhancements, upgrade instructions and caveats, resolved issues, and known issues for FortiADC™ D-Series Release 4.5.2, Build 597.

FortiADC D-Series provides load balancing, both locally and globally, and application delivery control.

For additional documentation, visit: http://docs.fortinet.com/fortiadc-d-series/.

What's new

This release includes the following major new features and enhancements:

Software OpenSSL library upgrade

- Software OpenSSL library has been upgraded to openssl-1.0.1s (the latest version) on all FortiADC platforms.
- It's fully functional on FortiADC software ONLY. (For information on hardware OpenSSL library upgrade, see"Known issues" on page 12.)

Enhanced Certificate validation

- Support for multiple Online Certificate Status Protocol (OCSP) setups.
- Support for multiple Certification Revocation List (CRL) files.

"Description" field for child records in Geo IP Whitelist

- Allows the user to add a brief notation for each child record added to a parent record.

US-Government (USG) Mode

- Allows the user to change the appliance from the default regular (REG) mode to USG mode via special license key.
- Locks the FortiADC D-Series appliance to servers located within the U.S. only.

For details on new features, see the *FortiADC Handbook*.

Hardware and VM support

FortiADC D-Series Release 4.5.2 supports the following hardware platforms:

- FortiADC 100F
- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D

FortiADC Release 4.5.2 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

Upgrade instructions

Use the following instructions to upgrade to 4.5.2.

Important: Before you perform an upgrade from any version earlier than the previous, read the release notes for past releases. Release notes include information about the changes introduced in those upgrades.

Supported upgrade paths

4.3.x to 4.5.x	Direct upgrade with the web UI or CLI.
4.2.x to 4.5.x	Direct upgrade with the web UI or CLI.
4.1.x to 4.5.x	You can upgrade from FortiADC 4.1.x using the CLI. Direct upgrade from 4.1.x to 4.5.x is not supported from the web UI. See the FortiADC Handbook for instructions on upgrading with the CLI.
4.0.x to 4.5.x	Direct upgrade from 4.0.x and earlier is not supported. You must first upgrade to FortiADC 4.1.x, and the system must be in an operable state.

See the release notes for earlier versions for guidance on those upgrades.

Upgrading a standalone appliance from release 4.2.x or later

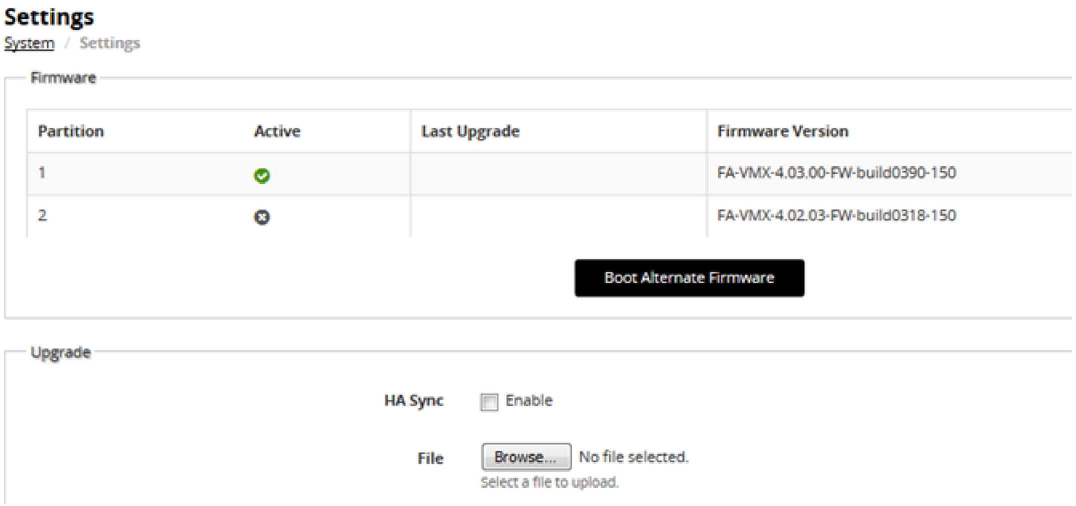
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- Updates the firmware on the inactive partition and then makes it the active partition.
- Copies the firmware on the active partition, upgrades it, and installs it in place of the configuration on the inactive partition.

For example, if partition 1 is active, and you perform the upgrade procedure:

- Partition 2 is upgraded and becomes the active partition; partition 1 becomes the alternate partition.
- The configuration on partition 1 remains in place; it is copied, upgraded, and installed in place of the configuration on partition 2.

This is designed to preserve the working system state in the event upgrade fails or is aborted.



Settings

System / Settings

Firmware

Partition	Active	Last Upgrade	Firmware Version
1	✓		FA-VMX-4.03.00-FW-build0390-150
2	✗		FA-VMX-4.02.03-FW-build0318-150

Upgrade

HA Sync □ Enable

File Browse... No file selected.

Select a file to upload.

Before you begin:

- You must have super user permission (user admin) to upgrade firmware.
- Download the firmware file from the Fortinet Customer Service & Support website: https://support.fortinet.com/
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

To update firmware:

1. Go to System > Settings.
2. Click the **Maintenance** tab.
3. Scroll to the Upgrade section.
4. Click **Browse** to locate and select the file.
5. Click ⬆ to upload the firmware and reboot.
   The system replaces the firmware on the alternate partition and reboots. The alternate (upgraded) partition becomes the active, and the active becomes the alternate.
6. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

Upgrading an HA cluster from release 4.3.x or later

The upgrade page for Release 4.3.0 and later includes an option to upgrade firmware on all nodes in a cluster from the primary node.

The following process occurs when you perform the HA upgrade procedure with this option:

1. The primary node pushes the firmware image to the member nodes.
2. The primary node notifies the member nodes of the upgrade, and it takes their user traffic during the upgrade.

3. The upgrade command is run on the member nodes, the systems are rebooted, and the member nodes send the primary node an acknowledgment that upgrade has been completed.
4. The upgrade command is run on the primary node, and it reboots. When the system is rebooting, a member node assumes primary status, and the traffic fails over from the former primary node to the new primary node.

After the upgrade process is completed, the system determines whether the original node becomes the primary node, according to the HA Override setting:

- If Override is enabled, the cluster considers the Device Priority setting. Both nodes usually make a second failover in order to resume their original roles.
- If Override is disabled, the cluster considers uptime first. The original primary node will have a smaller uptime due to the order of reboots during the firmware upgrade. Therefore it will not resume its active role; instead, the node with the greatest uptime will remain the new primary node. A second failover will not occur.

Before you begin:

- You must have super user permission (user admin) to upgrade firmware.
- Download the firmware file from the Fortinet Customer Service & Support website: https://support.fortinet.com/
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- Verify that the cluster node members are powered on and available on all of the network interfaces that you have configured. If required ports are not available, HA port monitoring could inadvertently trigger an additional failover, resulting in traffic interruption during the firmware update.
- You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

To update the firmware for an HA cluster:

1. Log into the web UI of the primary node as the admin administrator.
2. Go to System > Settings.
3. Click the **Maintenance** tab.
4. Scroll to the Upgrade section.
5. Click **Browse** to locate and select the file.
6. Enable the **HA Sync** option.
7. Click ⬆ to upload the firmware and start the upgrade process.
   To complete the upgrade, the system reboots and logs you out.
8. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

Note: Upgrade with HA Sync can take up to 10 minutes.

Web browsers

Release 4.5.2 has been tested with the following browser versions:

- Chrome Version 45.0.2454.85
- Firefox 40.0.3

If you use earlier versions and encounter issues with web UI expected behavior, try a tested browser version to see if it resolves the issue.

Resolved issues

This sections lists the major resolved issues in this 4.5.2 release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
380115	Sometimes, the system may fail due to slow OCSP response.
380102	In some cases, the system may fail to respond to client requests.
365394	Health status check on GSLB and LLB may not syn well, giving the wrong impression that the virtual server for GSLB is down.
377823	Inadvertent memory override may cause gicd crashes with global DNS configuration.
377812	The hardware SSL version may fail to download the entire file when downloading a large file from the appliance in a HTTPS to HTTP setup.
378860	TCP sessions could be wiped out after enabling SNAT and proximity route in Local Load Balancing.
377869	Unset OCSP URL may cause the CLI crash in some cases.
377698	Mismatching information in the SLB.elog may cause server validation failure.

Known issues

No new issues have been discovered in this 4.5.2 release. This section lists the major known issues carried over from the 4.5.1 release. For inquiries about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
	Hardware OpenSSL library upgrade is still pending development. As a result, the latest version of OpenSSL library (openssl-1.0.1s) is not fully functional on FortiADC hardware. **Workaround:** In order to use the latest OpenSSL library, be sure to disable Hardware SSL. Otherwise, the appliance will use the old OpenSSL library. For information on software OpenSSL library upgrade, see "What's new" on page 5.
241073	The SNMP agent will stop service about 4-5 seconds when there is an interface IP address change. Just wait for the process to complete.
291553	Unexpected behavior for the web UI with Internet Explorer. We recommend you use Chrome or Firefox to workaround this issue as we investigate it.
299578	Do not specify special characters for the configuration name for addresses, services, address groups, and service groups. Only A-Z, a-z, 0-9, _, and - are valid. The user interface should allow only valid characters.
302133	Sometimes, the interface secondary IP address in a VDOM configuration is not be synced from master to slave in HA AA-mode. As a workround, you can change the secondary IP address and then change it back, triggering the sync configuration operation a second time.
303839	The interface "allow access" settings do not work as expected when interfaces in multiple VDOMs have the same IP address. To avoid this issue, do not use the same IP address for interfaces in multiple VDOMs.
304959	In some cases, it can take up to 2 minutes to begin logging after traffic logging has been enabled for a virtual server.
305083	It takes about 2 seconds for the GLB configuration Respond Single Record option to take effect.

Bug ID	Description
305169	In heath check configurations you can specify port 0 to mean "use the port configured for the real server." This does not work for ssh. For ssh health checks, specify the appropriate port (usually port 22).
305463	Packet capture does not work for HA port haport0. To work around, use `diagnose sniffer packet` instead.
306626	In some cases, the client certificate verification fails unexpectedly with remote OCSP. To work around this issue, use CRL instead of OSCP.
306961	If you have enabled ssh for the management interface and cannot make an ssh connection to it after upgrade, run the upgrade a second time to resolve the issue.
306969	After upgrade, random characters are added to the radius server configuration name. For example, the configuration name `abc` becomes `abc_1_1aa9acd`. The configuration works as expected, but you might want to modify the configuration name. After you upgrade: 1. Clone the configuration and modify the name. 2. Delete the configuration with the undesirable name.
308858	SSH health checks can be unstable when there are hundreds of real server pool members or LLB-gateways to poll. If possible, use another type of health check for large pools.
309343	The new master device SNMP port loading time is too long (8 minutes), when transitioning from slave to master. This problem occurs when there is a large HA node IP address list.The SNMP process needs to wait for the entire HA node IP list to finish loading. Just wait for the process complete.
363687	The 4.5.0 image does not include WAF Bot Detection good_bot.rule and bad_bot.rule libraries. You must run an update to the latest WAF signature package to add the libraries.
365439	Need to wait 30 seconds for new detected packets if you unset proximity and then set it back. Just wait for the system to complete the process.

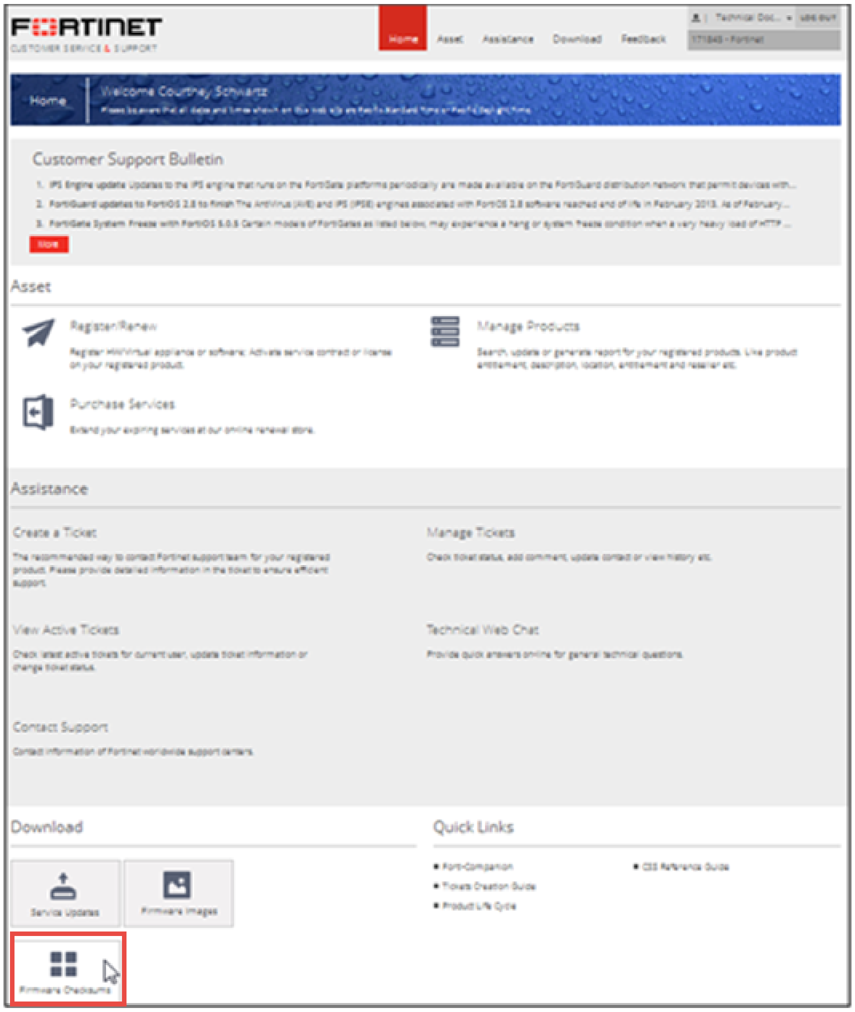
Bug ID	Description
366231	In HA A-A deployments, sometimes Layer 4 FTP persistence does not sync correctly. If this occurs, please try to initialize the FTP connection again.
367382	When there are more than 10,000 logs and you sort logs by OS type, it can take more than 15 minutes to display the log. Please wait for the system to complete the process.
367547	In VM deployments, Citrix Xen server supports 7 interfaces, and Xen project supports 8 interfaces. These are VM server limitations.
368009	When you disable and enable a WAF signature and reboot the system, the WAF signature might be missing in some rare cases. Please update the latest WAF signature when you encounter the problem.
368053	Import CRL via HTTP method does not work the URL points to an IPv6 http server. Only IPv4 is supported.
374051	If you reboot the switch when the device is starting up and joining the group, the workflow may get interrupted for a few seconds. **Workarund :** Disable the preempt on the traffic group or wait until the device becomes stable.
374468	Sometimes, the OSPF route table may become unstable when its neighbor has VRRP enabled. **Workaround:** Avoid using OSPF with VRRP for this release.
369990	The HC port may not be able to inherit the RS_port after config dest-addr. **Workaround**: Manually set the HC Por if you need to set the destination address.
366267	Two identical IPs may appear in 'get system traffic-goups-status details' in a situation where two virtual servers use the same VIP. **Note:** FortiADC sends one-time GARP redundantly. This is a normal device behavior, which bears no effect on its function.
372457	VRRP device with node_id=1 may send the GARP of virtual servers which not belong to its traffic group . **Note:** FortiADC sends one round ARP in non_switch_traffic_group redundantly. This is a normal device behavior, which bears no effect on its function.

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



Welcome Courtney Schwartz

Customer Support Bulletin

1. IPS Engine update Updates to the IPS engine that runs on the FortiGate platforms periodically are made available on the FortiGuard distribution network that permit devices with...
2. FortiGuard updates to FortiOS 2.8 to finish The AntiVirus (AVE) and IPS (IPSE) engines associated with FortiOS 2.8 software reached end of life in February 2013. As of February...
3. FortiGate System Freeze with FortiOS 5.0.5 Certain models of FortiGates as listed below, may experience a hang or system freeze condition when a very heavy load of HTTP ...

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.

Purchase Services

Extend your expiring services at our online renewal store.

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 online for general technical questions.

Contact Support

Contact information of Fortinet worldwide support centers.

Download

Quick Links

- Forti-Companion
- Tickets Creation Guide
- Product Life Cycle
- CSS Reference Guide

High Performance Network Security

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.