FortiADC D-Series Release Notes

Release 4.6.2

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

Friday, March 03, 2017

FortiADC D-Series Release Notes 4.6.2

Revision 1

TABLE OF CONTENTS

Change Log

Date	Change Description
01/06/2017	Initial release.
03/03/2017	Revision 1 to add Known Issue 410522.

Introduction

This document provides upgrade instructions, resolved issues, and known issues for FortiADC™ D-Series Release 4.6.2, Build 679.

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

FortiADC D-Series 4.6.2 is a patch release; no new features or enhancements are implemented in this release.

For product features, see the *FortiADC D-Series Handbook*.

Hardware and VM support

FortiADC D-Series Release 4.6.2 supports the following hardware platforms:

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

FortiADC Release 4.6.2 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 4.6.2.

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.
- Due to GUI upgrade, you may need to press **Ctrl+F5** to refresh the page if you encounter any display problem.
- When upgrading to 4.6.1, there may be a slight chance that the system may not load all ports correctly. If that happens, reboot FortiADC. All ports will be loaded correctly upon system reboot.

Supported upgrade paths

4.6.1 to 4.6.2	Direct upgrade via the web UI or CLI.
4.5.x to 4.6.x	Direct upgrade to FortiADC 4.6.0 from any version prior to 4.5.x is NOT supported via the GUI. The best way to upgrade is via the CLI using the `restore image` command. If you prefer to upgrade via the GUI, you must first upgrade the image to 4.5.x and then to 4.6.0. • GUI — Due to GUI changes in 4.6.0, make sure to refresh your browser when accessing the new FortiADC web GUI. • Global Load Balance — If your existing configuration contains the ISP feature, reconfigure it. This is because the ISP option has been moved. • HA —Update the firmware if HA sync is enabled. The process will take about 10 minutes to complete.
4.4.x to 4.5.x	Direct upgrade via the web UI or CLI.
4.3.x to 4.5.x	Direct upgrade via the web UI or CLI.
4.2.x to 4.5.x	Direct upgrade via 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

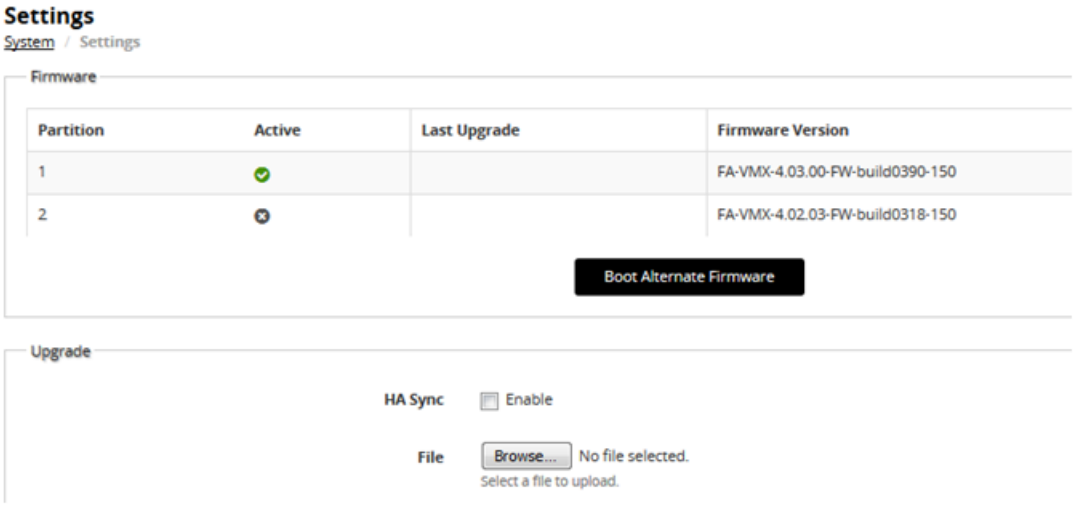
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- 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.



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 4.6.2 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 4.6.2 release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
400945	Setting cipher of real-server-profile as ECDHE or DHE may cause abnormal behavior in HTTPS load balance on platforms with hardware SSL acceleration cards.

Known issues

This section lists the major known issues in this FortiADC 4.6.2 release, including some remaining known issues carried over from 4.6.1 release. For inquiries about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
410522	Due to a change in IP pool name syntax restriction, some virtual server configurations could get lost when upgrading from 4.5.2 to 4.6.0 if the IP pool name contains a period (.). **Workaround**: Remove the period (.) or replace it with some other supported special character before upgrading.
387149	The Log Report table sometimes also show deleted virtual server data. **Workaround**: Execute the command "execute statistics-db sync " to clear the unwanted data.
233369	Shutting down the PPPoE interface sometimes may cause the default route to be deleted from the default route table. **Workaround**: Reconfigure the default route when shutting down the PPPoE interface.
380628	In VRRP mode, Global load-balance link member configuration sometimes cannot be fully synced to the slave. **Workaround**: Execute the command "execute ha force sync-config" to sync the configuration.
379236	Sometimes, the HA slave may still show "not sync" after you execute the command "execute ha force sync-config" in the master. **Workaround**: Clear the slave configuration, and execute "execute ha force sync-config" again.
377176	If the floating IP is the same as the interface IP, OSPF neighbor will not be built. **Workaround**: Avoid setting the floating IP the same as the interface IP.
376784	Some traffic log maybe missing when FortiADC is under heavy traffic stress. **Workaround**: Enable traffic log in suitable traffic stress; do not enable traffic log when CPU usage exceeds 60%.

Bug ID	Description
375487	The user is unable to delete the aggregate interface and its VLAN interface at the same time via the GUI. **Workaround**: Delete the VLAN interface first, and then the aggregate interface.
374286	Set SSL mirror-interface with an interface named # will make mirror fail. **Workaround**: Do not name an interface with #; use some meaningful string instead.
372459	Sometimes, the floating IP may be missing in the back end after some operations. **Workaround**: Reconfigure the floating IP.
368009	A signature may got lost after the user disables and enables it multiple times and reboots FortiADC. **Workaround**: Update the WAF signature package, and the signature will be added back to FortiADC.
366466	Sometimes, CPU usage may exceed 90% when you configure FortiADC too fast. **Workaround**: Normally, this lasts only a few seconds, and traffic will forward normally during the period. CPU usage will return to normal once the configuration is completed.
286360	Sometimes, you may not be able to create VIP rules in HA-AA mode. **Workaround**: Try to re-create it.
284972	When CPU is too busy, the "get system performance" command can't get CPU information. **Workaround**: Wait for a few seconds, and the system will get the information when the CPU becomes idle.
387745	When rebooting FortiADC under heavy traffic stress, it will take a few minutes for the system to resume forwarding all traffic. **Workaround**: Traffic will recover if you wait for a few minutes.
387149	The Log Report table may show deleted virtual server data. **Workaround**: Execute the "execute statistics-db sync " command to clear the deleted data.

Bug ID	Description
233369	Sometimes, shutting down the Point-to-Point Protocol over Ethernet (PPPoE) interface may lead to the default route being deleted from the default route table. **Workaround:** When shutting down the PPPoE interface, reconfigure the default route.
380628	In VRRP mode, Global-Load-Balance Link Member configuration sometimes cannot be fully synced to the slave. **Workaround:** Execute the "execute ha force sync-config" command to sync the configuration.
377176	If the floating IP is the same as the interface IP, The OSPF neighbor won't be built. **Workaround:** Avoid setting the floating IP the same as the interface IP.
375487	Can not delete the aggregate interface and its VLAN interface at the same time via GUI. **Workaround:** Delete the VLAN interface first, and then the aggregate interface.
374286	The command "set ssl-mirror-intf" with interface named # may not work. **Workaround:** Avoid using named interface "#"; use some meaningful string instead.
366466	Sometimes, FortiADC's CPU usage could exceed 90% if you configure the appliance rapidly. **Workaround:** Do nothing. This is because CPU usage could exceed 90% for only a few seconds during configuration. It will return to normal once the configuration is completed. Normally, traffic is still forwarded during the period.
286360	The VIP rules created in FortiADC sometimes do not work in HA-AA mode. **Workaround:** Re-create the rules again; they should work.
387745	If you reboot FortiADC under heavy traffic stress, it will take a few minutes for FortiADC to resume forwarding all traffic. **Workaround:** Wait for a few minutes until all traffic is recovered.
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.

Bug ID	Description
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.
305083	It takes about 2 seconds for the GLB configuration Respond Single Record option to take effect.
308858	SSH health checks can be unstable when there are hundreds of real server pool members or LLB-gateways to poll. **Workaround:** If possible, use another type of health check for large pools.
365439	Need to wait for 30 seconds for newly detected packets if you unset proximity and then set it back. **Workaround:** Just wait for the system to complete the process.
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. **Workaround:** Wait for the system to complete the process.
368053	Import CRL via HTTP method does not work with a URL pointing to an IPv6 HTTP server. **Workaround:** None. This feature applies to IPv4 only.
374468	Sometimes, the OSPF route table may become unstable when its neighbor has VRRP enabled. **Workaround:** Avoid using OSPF with VRRP.

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