FORTINET

High Performance Network Security

FortiADC™ D-Series Release Notes

VERSION 4.3.1

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

September 22, 2015

FortiADC™ D Series Release Notes 4.3.1

TABLE OF CONTENTS

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiADC™ Release 4.3.1, build 0397.

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

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

What's new

FortiADC Release 4.3.1 introduces the following new features:

- Virtual domains—Increased the maximum number of VDOMs on the following platforms:
  - FortiADC 700D – 30 VDOMs
  - FortiADC 1500D – 45 VDOMs
  - FortiADC 2000D – 60 VDOMs
  - FortiADC 4000D – 90 VDOMs
- Health checks— Added an HTTP CONNECT method health check, which is useful for testing the availability of web cache proxies.
- ISP address book—Added a province location setting to the ISP address book. The province setting is used in GSLB deployments in China to enable location awareness that is province-specific. For example, based on location, the DNS server can direct a user to a datacenter in Beijing or Guangdong rather than the broader location China. Only a predefined set of Chinese provinces is supported.

  When you upgrade to FortiADC version 4.3.1, the format of "restored" ISP files will be transformed into the new format and the province for all ISP subnets will be set to province `Unknown`. After you upgrade, you can export this file, edit it as needed, and then restore it.
- Advanced routing—Exception list for reverse path route caching.

For details, see the FortiADC Handbook.

Hardware model & VM support

FortiADC Release 4.3.1 supports the following platforms:

- FortiADC 200D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC-VM

Upgrade instructions

Use the following instructions to upgrade to 4.3.1.

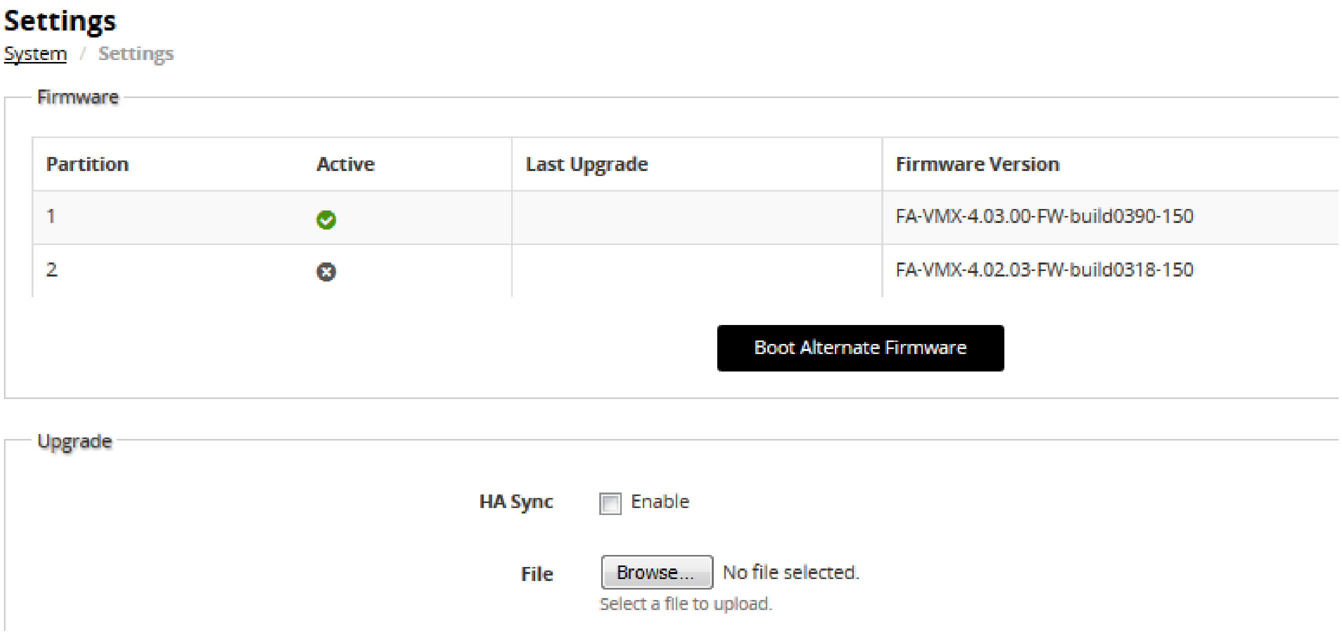
Important: Before you perform an upgrade from any version earlier than the previous, read the release notes for past releases. Release notes include information about the changes introduced in those upgrades.

Supported upgrade paths

4.3.0 to 4.3.1	Direct upgrade with the web UI or CLI.
4.2.x to 4.3.1	Direct upgrade with the web UI or CLI.
4.1.x to 4.3.1	You can upgrade from FortiADC 4.1.x using the CLI. Direct upgrade from 4.1.x to 4.3.x is not supported from the web UI. See the FortiADC Handbook for instructions.
4.0.x to 4.3.1	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 4.3.x

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. For example, if partition 2 is active, and you perform the upgrade procedure, partition 1 is upgraded and becomes the active partition; partition 2 becomes the alternate partition. The reason for this is to preserve the working system state in the event upgrade fails or is aborted.



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

HA Sync □ Enable

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.
- If you are upgrading from 4.2.x, make note of your HTTPS/TCPS profile SSL cipher suite configuration and LLB health check configuration. You might want to reconfigure them after the upgrade.
- 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.

If upgrading from 4.2.x:

1. The default SSL Ciphers list is different in 4.3.x. Go to Server Load Balance > Profile and review any HTTPS/TCPS profile configurations. Make any adjustments you find necessary.
2. The health checks for LLB link groups use the Shared Resources Health Check configuration in 4.3.x. Go to System > Shared Resources > Health Check and review the migrated health check configurations. Make any adjustments you find desirable.

Upgrading an HA cluster from release 4.3.x

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.
- If you are upgrading from 4.2.x, make note of your HTTPS/TCPS profile SSL cipher suite configuration and LLB health check configuration. You might want to reconfigure them after the upgrade.
- 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.

Web browsers

Release 4.3.1 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

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
260988	LLB now supports FTP active mode traffic.
269147	Dashboard throughput graphs are more reliable when the system is under heavy load.
275817	Added a route entry in the LLB gateway for health check packets. This resolves a reported issue with LLB health checks on a LACP interface using VLANs.
286635	The LLB source address hash method now works well.
287167	Improved the CLI configuration validation check for interface Secondary IP address settings.
287174	Resolved an issue with LLB virtual tunnel health checks in HA active-active deployments.
288525	The `execute backup log ftp` operation had failed unless the VDOM feature was enabled. The operation does not require VDOMs to be enabled.
289504, 289724	Resolved a memory-related issue with HA sync.
292064	An extraneous space in LDAP queries had caused authentication to fail.
292678	The 4.2.x to 4.3.0 upgrade removed configuration details if the real server pool configuration name had a period character. The period character was supported in 4.2.x and is supported in 4.3.1. If your real server pool configuration name has a period in it, we recommend that you not upgrade to 4.3.0. Instead, upgrade directly from 4.2.x to 4.3.1.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description

279780	High CPU utilization reported for Layer 7 HTTPS virtual servers on FortiADC hardware platforms. If you encounter this issue, use the CLI to disable hardware-based SSL acceleration.
	`FortiADC # config system global`
	`FortiADC (global) # set hardware-ssl disable`
	`FortiADC (global) # end`

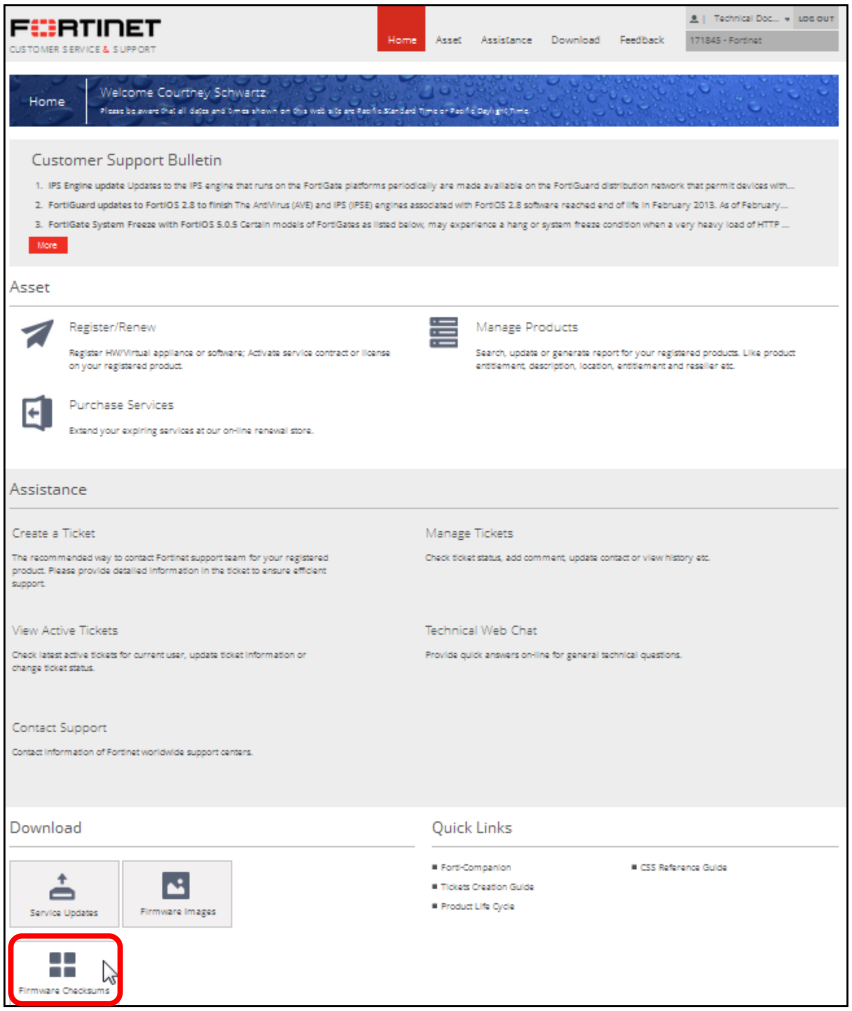
284963	Beginning with release 4.3.0, the health check configuration was moved to the Shared Resources section of the web UI and the `config system` section of the CLI. The upgrade migrates the configuration for SLB health checks and LLB health checks, but does not migrate LLB configurations with no health check members and does not migrate the LLB health check member source IP address because it is no longer used. We advise you to review your LLB health check configuration before and after the upgrade.
285780, 285781	If you downgrade from 4.3 to 4.2, some log files are erased. Back up log files before you downgrade.
287168	Beginning with release 4.3.0, in HTTPS/TCPS profiles, the default SSL ciphers list has changed and the upgrade changes the configuration to the new default list. If you want to preserve the list that is in your 4.2 configuration, you must reconfigure it after you upgrade.
288696	Beginning with release 4.3.0, the Global DNS Server > Global DNS Policy > Load Balance Pool configuration is no longer used in the GSLB framework. Upon upgrade, this configuration is deleted. Refer to the handbook to learn how to configure virtual server pools for the new GSLB framework.
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.
292171	Limitation: Due to firewall changes introduced in 4.3.0, a network interface and a virtual server must not have the same IP address.

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

Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time.

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 on-line 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 on-line 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