APPLICATION DELIVERY CONTROLLER

# FortiADC™ 3.1

## Release Notes

for D Series Models & FortiADC-VM

FortiADC™ 3.1 Release Notes for D Series Models & FortiADC-VM

December 5, 2013

Revision 1

| | |
|---|---|
| Technical Documentation | http://help.fortinet.com |
| Knowledge Base | http://kb.fortinet.com |
| Forums | https://support.fortinet.com/forums |
| Customer Service & Support | https://support.fortinet.com |
| Training | http://training.fortinet.com |
| FortiGuard Threat Research & Response | http://www.fortiguard.com |
| License Agreement | http://www.fortinet.com/doc/legal/EULA.pdf |
| Document Feedback | Email: techdocs@fortinet.com |

# Table of contents

# Introduction

This document provides a list of new/changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiADC™ 3.1 build 0094 for D series models and FortiADC-VM.

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

For additional documentation, please visit:

http://help.fortinet.com/fadc.html

# What’s new

Before upgrading, review the following **changes** for impact to your unique network.

## Custom error page

A custom error page can be uploaded to FortiADC to serve back to clients when layer 7 servers are unavailable

## Full NAT mode for Layer 4 load balancing

Layer 4 load balancing now supports Full NAT mode. FortiADC can now forward connections to back end servers using a definable source IP pool.

## Backup Server

A server can now be defined as 'Backup server'. FortiADC will forward traffic to it only when the rest of the servers in the pool are unavailable.

## Log Cache memory

In order to avoid hard disk wear and tear FortiADC allows logging to memory cache and writing logs to disk in bulk. Instead of writing to disk every log instantaneously use the CLI commands to write logs in bulk -

```
set event-log-cached-lines (100)
set traffic-log-cached-lines (10)
```

## Health check status sync for IPv6

Health check status of layer 4, IPv6 enabled virtual servers is now synched from maser to slave node.

# Upgrade instructions

## Hardware model & VM support

FortiADC™ 3.1 for D series models supports:

- FortiADC 200D
- FortiADC-VM

## Upgrading from release 3.0

To upgrade from FortiADC 3.0 use the web UI Backup and Restore tab or upgrade from CLI via SSH/Telnet.

## Upgrading from release 2.0

Upgrading from FortiADC 2.0 using the web UI or CLI via SSH/Telnet is not supported. Instead, to upgrade, **back up your configuration first**, perform a clean install using a TFTP server and connection to the console, then restore your configuration.

Unlike updating firmware, restoring firmware re-images the boot device ***before*** the operating system is loaded. Also, restoring firmware can only be done during a boot interrupt, before network connectivity is available, and therefore ***requires a local console connection to the CLI. It cannot be done through an SSH or Telnet connection.***

Alternatively, if you cannot physically access the appliance’s local console connection, connect the appliance’s local console port to a terminal server to which you have network access. Once you have used a client to connect to the terminal server over the network, you will be able to use the appliance’s local console through it. However, be aware that from a remote location, you may not be able to power cycle the appliance if abnormalities occur.

**To perform a clean install**

Back up your configuration before beginning this procedure, if possible. Restoring firmware resets the configuration, including the IP addresses of network interfaces. For information on backups, see the FortiADC Handbook. For information on reconnecting to a FortiADC appliance whose network interface configuration was reset, see the FortiADC Handbook.

1. Download the firmware file from the Fortinet Technical Support web site:

   https://support.fortinet.com/

2. Connect your management computer to the FortiADC console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a ***local console connection*** from your management computer to the CLI of the FortiADC appliance, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read-Write* permissions in the *Maintenance* category. For details, see the FortiADC Handbook.

4. Connect port1 of the FortiADC appliance directly or to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as `tftpd` (Windows, Mac OS X, or Linux) on your management computer.)

Because TFTP is ***not*** secure, and because it does not support authentication and could allow anyone to have read and write access, you should ***only*** run it on trusted administrator-only networks, ***never*** on computers directly connected to the Internet. If possible, immediately turn off `tftpd` off when you are done.

7. Verify that the TFTP server is currently running, and that the FortiADC appliance can reach the TFTP server.

   To use the FortiADC CLI to verify connectivity, enter the following command:

   ```
   execute ping 192.168.1.168
   ```

   where `192.168.1.168` is the IP address of your TFTP server.
8. Enter the following command to restart the FortiADC appliance:

   ```
   execute reboot
   ```

   As the FortiADC appliances starts, a series of system startup messages appear.

   Press any key to display configuration menu........
9. Immediately press a key to interrupt the system startup.

   You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiADC appliance reboots and you must log in and repeat the `execute reboot` command.

   If you successfully interrupt the startup process, the following messages appears:

   ```
    [G]:  Get firmware image from TFTP server.
    [F]:  Format boot device.
    [B]:  Boot with backup firmware and set as default.
    [Q]:  Quit menu and continue to boot with default firmware.
    [H]:  Display this list of options.

   Enter G,F,B,Q,or H:

   Please connect TFTP server to Ethernet port "1".
   ```
10. Type `G` to get the firmware image from the TFTP server.

    The following message appears:

    ```
    Enter TFTP server address [192.168.1.168]:
    ```
11. Type the IP address of the TFTP server and press Enter.

    The following message appears:

    ```
    Enter local address [192.168.1.188]:
    ```
12. Type a temporary IP address that can be used by the FortiADC appliance to connect to the TFTP server.

    The following message appears:

```
Enter firmware image file name [image.out]:
```

**13.** Type the file name of the firmware image and press Enter.

The FortiADC appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
MAC:00219B8F0D94

###########################

Total 28385179 bytes data downloaded.

Verifying the integrity of the firmware image..

Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?
```

If the download fails after the integrity check with the error message:

```
invalid compressed format (err=1)
```

but the firmware matches the integrity checksum on the Fortinet Technical Support web site, try a different TFTP server.

**14.** Type `D`.

The FortiADC appliance downloads the firmware image file from the TFTP server. The FortiADC appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection.

The FortiADC appliance reverts the configuration to default values for that version of the firmware.

**15.** To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

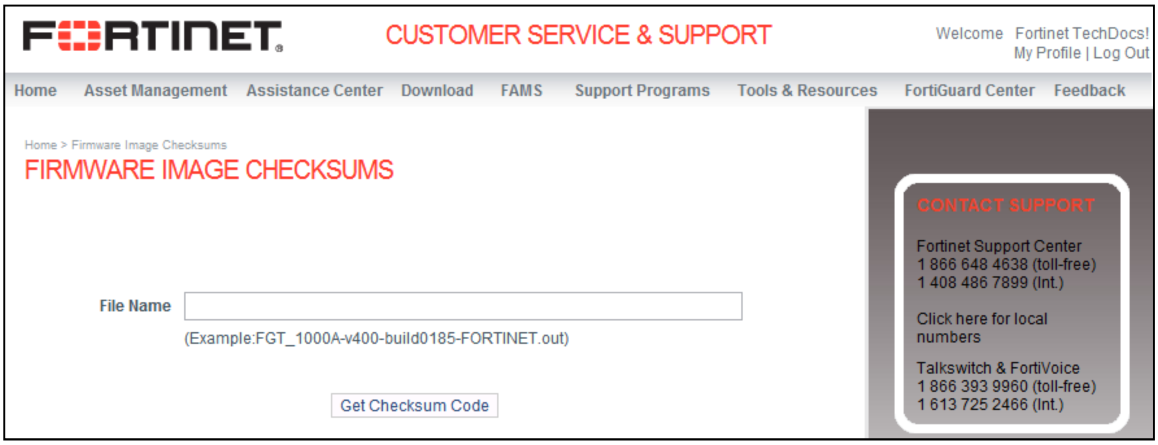
The firmware version number is displayed.

**16.** Either reconfigure the FortiADC appliance or restore the configuration file. For details, see the FortiADC Handbook.

## 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, go to *Download* > *Firmware Image Checksums*. In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.



FIRMWARE IMAGE CHECKSUMS

File Name

(Example:FGT_1000A-v400-build0185-FORTINET.out)

Fortinet Support Center
1 866 648 4638 (toll-free)
1 408 486 7899 (Int.)

Click here for local numbers

Talkswitch & FortiVoice
1 866 393 9960 (toll-free)
1 613 725 2466 (Int.)

# 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 |
|---|---|
| 0208479 | Access Profile is not correctly mapped to the latest GUI tree |
| 0212389 | When LLB health check is enabled traffic originating from FortiADC does not use the correct interface |
| 0210682,<br>0199410 | Problems accessing the HTTP virtual server when DoS Protection is enabled |
| 0192961 | Source-IP and hash-IP persistence do not work correctly |
| 0212239 | Empty 'Certificate Verify' in HTTPS virtual server causes a restart |
| 0210840 | L7 virtual server crashes when oscp_url is set with a IPv6 address |
| 0210684 | Report browse page cannot be displayed after running a report |
| 0210994 | Report crashes when the report configuration has' Additional Information' attached |
| 0208480 | VLAN and aggregated interfaces cannot be chosen in QoS 'root-queue' |
| 0207496 | QoS “root queue” does not work in VLAN/aggregated interfaces |
| 0207490 | QoS IP-range not working |

# 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 |
|---|---|
| 0224253 | The virtual server statistic files fills up the /tmp space |
| 0216943 | Daemon 'update' continuously sending DNS requests |
| 0209152 | Response delays when Syn Cookie is enabled and DDoS attack is in progress |
| 0222675 | When LLB and rt-cache-reverse are enabled traffic can be routed via reverse interface even when there's no route defined |
| 0221177 | Cannot change an existing 'destination' entry to blank in Policy Route |
| 0220531 | QoS not working properly when using ip-range |
| 0219247 | Changing QoS configuration can cause existing sessions to hang for several seconds |
| 0209896 | FTP data connections hang |
| 0222414 | Adding a new LLB gateway or enabling/disabling an interface effects existing traffic |
| 0224375 | Incorrect LLB source NAT when traffic rebalanced upon gateway re-balancing |
| 0214421,<br>0224242 | Issues viewing logs after generating a report |
| 0223699 | System time does not correctly sync to the slave node |
| 0223497 | L7 persistence information does not sync to slave node after failover |
| 0208499 | Configuration restore does not work properly in HA clusters |
| 0220819 | Subtype column filter in log tab does not filter correctly |
| 0221002 | Protocol column filter in log tab does not work |
| 0210637 | Upgrade from v2.0 might crash the system |
| 0194525 | HA slave flash drive deleted |
| 0204359 | NTLM authentication fails |

| | |
|---|---|
| 0209761 | IPv6 connection limit fails when output interface set to ‘all’ |
| 0208497 | All nodes will stay in salve node if their age is the same and override is disabled |
| 0208499 | HA configuration restore function does not work properly |
| 0207477 | ‘Unset monitor’ fails in HA mode |