FortiDDoS 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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

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

Tuesday, July 18, 2017

FortiDDoS 4.3.1 Release notes

Revision 3

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-03-05	Initial release for version 4.3.1
2017-04-05	Revision 2 with updates in 'Common Vulnerabilities and Exposures' table.
2017-07-17	Revision 3 with updates in the section: Upgrading

Introduction

This document provides a list of new/changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiDDoS 4.3.1 build 0416. The TP2ASIC version is 43010090. Date: May 3, 2017.

FortiDDoS is a network behavior anomaly (NBA) prevention system that detects and blocks network attacks that are characterized by excessive use of network resources. These attacks are known as distributed denial of service (DDoS) attacks.

For additional documentation, please visit:

http://docs.fortinet.com/fortiddos

What's new

FortiDDoS 4.3.1 release includes the below change:

Mantis ID	Description
412904	FortiDDoS Cloud Monitoring program is End of Life and options related to Cloud Monitoring have been removed.

Hardware support

This release supports the following hardware models:

- FortiDDoS 200B
- FortiDDoS 400B
- FortiDDoS 600B
- FortiDDoS 800B
- FortiDDoS 900B
- FortiDDoS 1000B
- FortiDDoS 1000B-DC
- FortiDDoS 1200B
- FortiDDoS 2000B
- FortiDDoS 2000B-USG

FortiDDoS A series models are not supported.

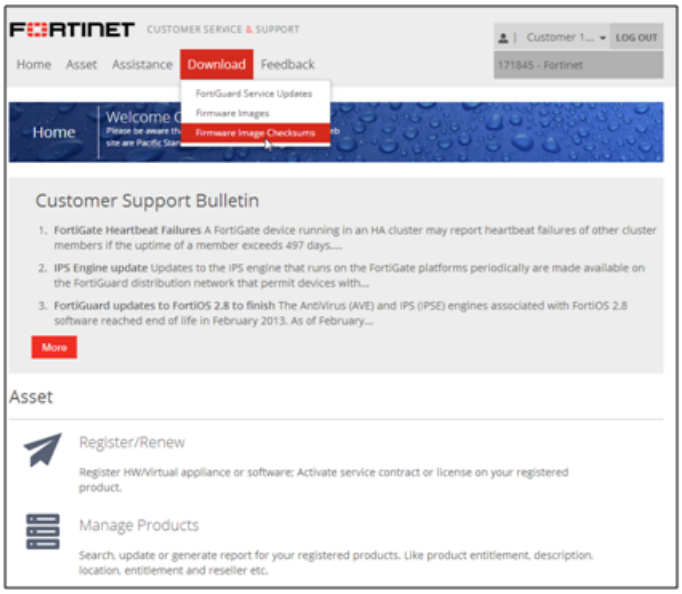
Image checksums

To verify the integrity of the firmware file, use a checksum tool to 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 software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

Figure 1: Customer Service & Support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, and then click **Firmware Image Checksums**.

Alternatively, near the bottom of the page, click the **Firmware Image Checksums** button. (The button appears only if one or more of your devices have a current support contract.) In the Image File Name field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading

Note: **FortiDDoS takes longer to upgrade than x86-based systems. Prepare your maintenance window to accommodate at least 20 minutes for the upgrade (most will not take this long but some may). In some cases, you need to upgrade to an intermediate release before the final upgrade (2 x 20 minutes). Plan accordingly, after you understand the upgrade path from the table below. We strongly recommend that while you can upgrade via GUI, you also connect to the console port, which will provide status messages during the upgrade process, while the GUI is offline.**

Supported upgrade paths

Use the following instructions to upgrade to FortiDDoS 4.3.1.

Steps	Current Release	Upgrade method	Upgrade path
1	<4.1.5	BIOS ONLY	1. Upgrade to 4.1.5. 2. Upgrade to 4.2.3. Follow Step 2. 3. Upgrade to 4.3.1. Follow Step 3. Refer to section 3 for detailed upgrade procedure.
2	4.1.5 to 4.2.2	GUI/CLI/BIOS	1. Upgrade to 4.2.3. 2. Upgrade to 4.3.1. Follow Step 3. Refer to sections 1, 2 and 3 for detailed upgrade procedure. If desired, create a new SPP for DNS servers. Allow the system to operate for one week (recommended) and then generate traffic Statistics for all active SPPs (even if new DNS SPP was not created). Run System Recommendations to set new System Recommended Thresholds. We suggest you place SPPs into Detection Mode for several hours to days to monitor for false-positives, then tune Thresholds and place SPPs into Prevention Mode.

Steps	Current Release	Upgrade method	Upgrade path
3	4.2.3 to 4.3.0	GUI/CLI/BIOS	• Upgrade directly to 4.3.1. Refer to sections 1, 2 and 3 for detailed upgrade procedure. In 4.3.x, a new Method Per Source Scalar has been added to all SPPs. After upgrading, there will be no Threshold for these. We suggest to allow the system to operate for one week after upgrade, then generate Traffic Statistics and view the Method Per Source Scalar. Either manually set this Threshold by multiplying the Inbound Traffic measurement by three and entering that number in the Threshold or run System Recommendations for all thresholds. If you create new System Recommendations, we suggest to place the SPPs into Detection mode for a few days and review drops for false positive errors.

Note the following:

- If you are upgrading via BIOS, failure to follow the upgrade path will result in the loss of system configuration and all stored data for graphs and reports.
- Upgrading FortiDDoS takes significantly longer than x86-based systems. For upgrading from the GUI, we recommend connecting a console as well, which will allow you to see upgrade information during the process. Otherwise please expect >15 minutes for an upgrade - the time will vary depending on the number of TP2 processors in the appliance.
- To track the progress of upgrade from any version, check the console and once the upgrade is done, clear your browser cache and refresh.
- FortiDDoS 4.2.0 and later releases adds additional parameter monitoring and Thresholds for DNS Features. When upgrading from Releases prior to 4.2.0, in order to activate these Thresholds, FortiDDoS needs to operate for several hours to several days. Then you need to run Traffic Statistics Reports and System Recommendations to create Thresholds. It is recommended that DNS servers be placed in a separate SPP to facilitate this.
- If you have Asymmetric Traffic, allow the system to operate for at least 8 days after upgrade, then re-run 1-week Traffic Statistics and System Recommendations. This will modify the TCP High Port Thresholds to improve graphing and responsiveness. This is required even though you may have followed instructions to re-run Traffic Statistics as part of the upgrade process.
- For FortiDDoS 4.2.x, the SPP Statistics shows data for packets/period while 4.3.x shows packets/sec. So the same level of traffic data shown in 4.2.x and 4.3.x would be different.

Prerequisites

- The procedures explain the upgrade from 4.2.3. If your system is not at 4.2.3, please refer to the table above and follow the instructions.
- Download the 4.3.1 firmware file from the Fortinet Technical Support website: https://support.fortinet.com/.
- Check that the upgrade info file is available on your FortiDDoS system:

- On the System Status page, click on the CLI Console window to connect and see the # prompt.
- Enter: `f cat /var/log/upgrade_info.txt`
- If you do not see 4,2,0 or 4,2,1, followed by the system Serial Number or Host Name and # prompt, check which Release is showing in the System Summary page and if 4.2.0, or 4.2.1 is showing, contact Fortinet support. This file is needed to properly upgrade your system.

  Examples:

  4,2,0`FI800B3913000013 #`
  4,2,1`FDD-169 #`

- **Back up your configuration before beginning this procedure:**
  - If you later revert to an earlier firmware version, the active configuration is deleted, and you will want to restore the configuration that worked well with the earlier version.
  - Attempting to use a system configuration from a newer firmware release on a downgraded firmware release may have unexpected results.
- Make a note of configuration items that are disabled in your active configuration. Configurations that are not enabled are not preserved in the upgrade to 4.2.3. For example, if a custom HTTP service port, log remote port, or event log port have been configured and then disabled in an earlier version, the configuration information is not preserved in the upgrade to 4.2.3.
- You must have super user permission (user admin) to upgrade firmware.
- After upgrade you may need to regenerate system recommended Thresholds. If so, record any manually-set Thresholds before upgrading so you can re-enter these after new Thresholds have been set.

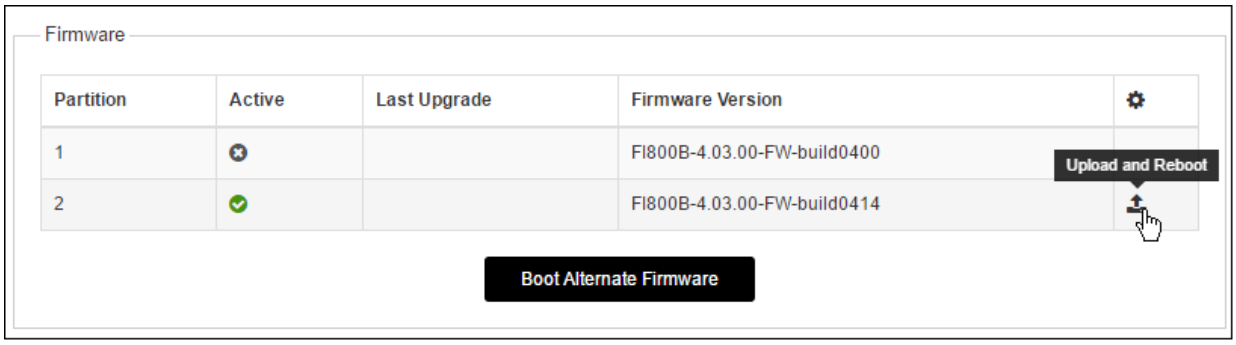
Section 1: Upgrading using GUI

Ensure that you have read the general Upgrading section before you start an upgrade.

Note: You can upgrade directly to FortiDDoS 4.3.1 via GUI from any version above 4.2.3. For any version below 4.2.3, you MUST upgrade to 4.2.3 and then to 4.3.1.

The following figure shows the user interface for managing firmware.

For this upgrade, you must use Partition 2.



To install firmware:

1. Go to **System** > **Maintenance** > **Backup & Restore** tab.
2. Under Firmware Upgrade/Downgrade, in the row for Partition 2, click the Upload and Reboot icon to display the upload file controls.
3. Use the upload file controls to select the firmware image file.
4. Click **OK** to upload the file, install the firmware, and restart the system. Always use Partition 2 for upgrades even if Partition 2 is showing a newer Release than Partition 1. From 4.2.3, partition choices will not be shown.

   WARNING: **The reboot takes several minutes (as many as 15) – longer for larger systems and there is no progress indicator on the GUI.** FortiDDoS must write register information to each TP2 which takes considerably longer than simply loading x86 firmware as in most systems. This is only a factor in the upgrade reboot. Once installed, the TP2 firmware is persistent and will only change with a further upgrade. **It is very important the system not be disturbed or power cycled during this process.** A power cycle will result in an unusable system that must be returned to factory for repair. Ideally, leave the system for 20 minutes. If the system has NOT recovered in that time, contact Fortinet Support.
5. Clear your browser cache to avoid potential issues that can be caused by caching.

   During upgrade, the console will show upgrade progress information if a terminal is connected to it. See the Sample console log for reference.
6. Login and from **Dashboard**, confirm that the firmware version is correct.

Section 2: Upgrading via CLI

Ensure that you have read the general Upgrading section before you start an upgrade.

Note: You can upgrade directly to FortiDDoS 4.3.1 via CLI from any version above 4.1.5. For any version below 4.1.5, you MUST upgrade to 4.1.5 and then to 4.3.1.

To install firmware:

1. Connect your management computer to the FortiDDoS console port using an RJ-45-to-DB-9 serial cable or a null-modem cable. Use the following terminal settings:
   Speed (Baud Rate): 9600 Data Bits: 8 Stop Bits: 1 Parity: None
2. Initiate a connection to the CLI and log in as the user admin.
3. Use an Ethernet cable to connect FortiDDoS mgmt1 to the TFTP server directly, or connect it to the same subnet as the TFTP server.
4. If necessary, start the TFTP server.
5. Enter the following command to transfer the firmware image to the FortiDDoS system:
   ```
   execute restore image tftp <filename_str> <tftp_ipv4>
   ```
   where <filename_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:
   ```
   execute restore image tftp image.out 192.168.1.168
   ```
   The following message appears:
   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
6. Type y.
   The system gets the image from the TFTP server, installs the firmware, and restarts.

   See the Sample console log for reference.

   WARNING: **The reboot takes several (as long as 15) minutes – longer for larger systems** (see the progress examples from the console output below). FortiDDoS must write register information to each TP2 which takes considerably longer than simply loading x86 firmware as in most systems. This is only a factor in the upgrade reboot. Once installed, the TP2 firmware is persistent and will only change with a further upgrade. **It is very important the system not be disturbed or power cycled during this process.** A power cycle will result in an unusable system that must be returned to factory for repair. Ideally, leave the system for 20 minutes. If the system has NOT recovered in that time, contact Fortinet Support.

- To verify that the firmware was successfully installed, login and use the “get system status” command, confirming the version information is correct:

```
Version: FortiDDoS-900B v4.3.0,build0416,170304
TP2ASIC Version: 43010090 Date: Feb 21, 2017
IP Reputation DB: Not enabled
Serial-Number: FI900B3915000043
BIOS version: 05000002
Log disk: Capacity 62 GB, Used 1 GB ( 2.74%), Free 61 GB
RRD disk: Capacity 369 GB, Used 164 GB (44.54%), Free 204 GB
```

```
Hostname: FI900B3915000043
HA configured mode: standalone
HA effective mode: standalone
Distribution: International
License Type: -
Uptime: 0 days 4 hours 2 minutes
Last reboot: Mon Mar 06 10:59:22 PST 2017
System time: Mon Mar 06 15:02:03 PST 2017
```

- **IMPORTANT**: Releases 4.1.6, 4.1.8 and 4.2.0 included improvements to system recommended thresholds and threshold ranges. If you upgraded from any release lower than 4.2.0, take the following additional steps after the upgrade to 4.2.3 has completed and the system has restarted:
  - If you now have a DNS SPP, you will need to leave that SPP in learning mode (no Thresholds and in Detection mode only) for as long as possible (1 week recommended). After one week you can run Traffic Statistics and set thresholds, as well as configure DNS Features and Anomaly settings. Then run for another week in Detection mode to check that Thresholds and settings are correct.
  - For every other SPP, immediately enter the following commands to re-generate traffic statistics over the longest period of known “clean” traffic:

    ```
    config spp
    edit <spp_name>
    config ddos spp threshold-report
    set generate enable
    set report-period {last-hour | last-8-hours | last-24-hours | last-week |
    last-month | last-year}
    end
    ```
  - Create System Recommendation with the following commands:

    ```
    config spp
    edit <spp_name>
    config ddos spp threshold-adjust
    set threshold-adjustment-type system-recommendation
    set threshold-system-recommended-report-period
    {1-hour | 8-hours | 1-day | 1-week | 1-month | 1-year}
    ```
  - Re-enter the manual threshold settings you want to continue using from your previous configuration. See Thresholds for commands.

Section 3: Upgrading via BIOS

Ensure that you have read the general Upgrading section before you start an upgrade.

Note: You can upgrade directly to FortiDDoS 4.3.1 via BIOS from any version above 4.1.5. For any version below 4.1.5, you MUST upgrade to 4.1.5 and then to 4.3.1.

The system configuration will be lost when upgrading using BIOS. For this reason, BIOS upgrade should only be used for upgrading new systems that have not been put in service.

If you want to delete customer configuration and traffic data from a system, use CLI commands "`formatlogdisk`" and "`factory default`".

To upgrade the firmware:

1. Download the new firmware image.
2. Copy the file to a location you can access from the FortiDDOS appliance using TFTP.
3. Connect to the FortiDDOS appliance console.
4. Reboot the system and, when prompted, press any key to display the BIOS configuration menu.
5. Select option G so that the system can get the new firmware image from the TFTP server and load it when it reboots.
   The following example shows the CLI sequence:

```
FI-1KBXXXXXXXXX # exe reboot This operation will reboot the system ! Do you want to
continue? (y/n) y
System is rebooting... The system is going down NOW !!
Please stand by while rebooting the system.
FortiDDoS-1000B (19:35-09.19.2013)
Ver:04000005
Serial number:FI1KBXXXXXXXXX
RAM activation
CPU(00:000306a9 bfebfbff): MP initialization
CPU(01:000306a9 bfebfbff): MP initialization
CPU(02:000306a9 bfebfbff): MP initialization
CPU(03:000306a9 bfebfbff): MP initialization
CPU(04:000306a9 bfebfbff): MP initialization
CPU(05:000306a9 bfebfbff): MP initialization
CPU(06:000306a9 bfebfbff): MP initialization
CPU(07:000306a9 bfebfbff): MP initialization
Total RAM: 8192MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
...
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.

Enter Selection [G]:

Please connect TFTP server to Ethernet port "MGMT".

Enter TFTP server address [192.168.1.168]: 192.168.1.168
Enter local address [192.168.1.188]: 192.168.1.188
Enter firmware image file name [image.out]: FDD_1000B-v400-build0416-FORTINET.out
MAC:085B0E9F061C
#################################################################
Total 76694566 bytes data downloaded.

Verifying the integrity of the firmware image.
Total 204800kB unzipped.
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?d
Programming the boot device now.
.....................................................................................
.....................................................................................
..................
Reading boot image 2791231 bytes.
Initializing FortiDDoS...
System is started.
```

6. Set the management port IP address and gateway IP address using the console.
7. If you saved and edited the configuration file, restore it using the CLI or web UI.
8. If you did not save a configuration file, you must reconfigure the user accounts and system options.

Sample console log

Sample console log while upgrading from 4.3.0 to 4.3.1:

```
FI1K2B3915000007 # execute restore image tftp FDD_1200B-v400-
build0416-FORTINET.out 172.30.153.105
This operation will replace the current firmware version!
Do you want to continue? (y/n)y
Connect to tftp server 172.30.153.105 ...
Please wait...
#################################################################################
##############################
Get image from tftp server OK.
Verifying the integrity of the firmware image.FI1K2B3915000007 #
The system begins to upgrade ...
Firmware upgrade in progress ...
New image: FI1K2B-4.03.01-FW-build0416-170427
Done. 2
The system is going down NOW !!
Please stand by while rebooting the system.
FortiDDoS-1200B ( 8:27-10.26.2015)
Ver:05000002
Serial number:FI1K2B3915000007
RAM activation
CPU(00:000206d7 bfebfbff): MP initialization
CPU(01:000206d7 bfebfbff): MP initialization
CPU(02:000206d7 bfebfbff): MP initialization
CPU(03:000206d7 bfebfbff): MP initialization
CPU(04:000206d7 bfebfbff): MP initialization
CPU(05:000206d7 bfebfbff): MP initialization
CPU(06:000206d7 bfebfbff): MP initialization
CPU(07:000206d7 bfebfbff): MP initialization
CPU(08:000206d7 bfebfbff): MP initialization
CPU(09:000206d7 bfebfbff): MP initialization
CPU(0a:000206d7 bfebfbff): MP initialization
CPU(0b:000206d7 bfebfbff): MP initialization
Total RAM: 32768MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
......
Reading boot image 3712988 bytes.
Initializing FortiDDoS...\ufffd

System is started.
Updating Factory Image
FortiASIC-TP.4: update started. Reconfigure process takes a few minutes
FortiASIC-TP.5: update started. Reconfigure process takes a few minutes
FortiASIC-TP.1: update started. Reconfigure process takes a few minutes
```

```
FortiASIC-TP.0: update started. Reconfigure process takes a few minutes
FortiASIC-TP.1: 0% Complete
FortiASIC-TP.0: 0% Complete
FortiASIC-TP.5: 10% Complete
FortiASIC-TP.3: 10% Complete
FortiASIC-TP.5: 20% Complete
FortiASIC-TP.4: 10% Complete
FortiASIC-TP.0: 10% Complete
FortiASIC-TP.1: 10% Complete
FortiASIC-TP.3: 20% Complete
FortiASIC-TP.5: 30% Complete
FortiASIC-TP.4: 20% Complete
FortiASIC-TP.2: 10% Complete
FortiASIC-TP.0: 20% Complete
FortiASIC-TP.1: 20% Complete
FortiASIC-TP.3: 30% Complete
FortiASIC-TP.5: 40% Complete
FortiASIC-TP.4: 30% Complete
FortiASIC-TP.2: 20% Complete
FortiASIC-TP.0: 30% Complete
FortiASIC-TP.1: 30% Complete
FortiASIC-TP.3: 40% Complete
FortiASIC-TP.5: 50% Complete
FortiASIC-TP.4: 40% Complete
FortiASIC-TP.2: 30% Complete
FortiASIC-TP.0: 40% Complete
FortiASIC-TP.1: 40% Complete
FortiASIC-TP.3: 50% Complete
FortiASIC-TP.5: 60% Complete
FortiASIC-TP.4: 50% Complete
FortiASIC-TP.2: 40% Complete
FortiASIC-TP.0: 50% Complete
FortiASIC-TP.1: 50% Complete
FortiASIC-TP.3: 60% Complete
FortiASIC-TP.5: 70% Complete
FortiASIC-TP.4: 60% Complete
FortiASIC-TP.2: 50% Complete
FortiASIC-TP.0: 60% Complete
FortiASIC-TP.1: 60% Complete
FortiASIC-TP.3: 70% Complete
FortiASIC-TP.5: 80% Complete
FortiASIC-TP.4: 70% Complete
FortiASIC-TP.2: 60% Complete
FortiASIC-TP.0: 70% Complete
FortiASIC-TP.1: 70% Complete
FortiASIC-TP.3: 80% Complete
FortiASIC-TP.5: 90% Complete
FortiASIC-TP.4: 80% Complete
FortiASIC-TP.2: 70% Complete
FortiASIC-TP.0: 80% Complete
FortiASIC-TP.1: 80% Complete
FortiASIC-TP.3: 90% Complete
FortiASIC-TP.5: FPGA image download complete.
FortiASIC-TP.5: Checking update image on FPGA.....
FortiASIC-TP.5: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.5: UPDATE FPGA OK, WAIT FOR REBOOT....
```

```
FortiASIC-TP.4: 90% Complete
FortiASIC-TP.2: 80% Complete
FortiASIC-TP.0: 90% Complete
FortiASIC-TP.1: 90% Complete
FortiASIC-TP.3: FPGA image download complete.
FortiASIC-TP.3: Checking update image on FPGA.....
FortiASIC-TP.3: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.3: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.4: FPGA image download complete.
FortiASIC-TP.4: Checking update image on FPGA.....
FortiASIC-TP.4: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.4: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.2: 90% Complete
FortiASIC-TP.0: FPGA image download complete.
FortiASIC-TP.0: Checking update image on FPGA.....
FortiASIC-TP.0: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.0: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.0: update finished
FortiASIC-TP.1: FPGA image download complete.
FortiASIC-TP.1: Checking update image on FPGA.....
FortiASIC-TP.1: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.1: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.1: update finished
FortiASIC-TP.2: FPGA image download complete.
FortiASIC-TP.2: Checking update image on FPGA.....
FortiASIC-TP.2: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.2: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.2: update finished
FortiASIC-TP.3: update finished
FortiASIC-TP.4: update finished
FortiASIC-TP.5: update finished
FortiDDoS-1200B ( 8:27-10.26.2015)
Ver:05000002
Serial number:FI1K2B3915000007
RAM activation
CPU(00:000206d7 bfebfbff): MP initialization
CPU(01:000206d7 bfebfbff): MP initialization
CPU(02:000206d7 bfebfbff): MP initialization
CPU(03:000206d7 bfebfbff): MP initialization
CPU(04:000206d7 bfebfbff): MP initialization
CPU(05:000206d7 bfebfbff): MP initialization
CPU(06:000206d7 bfebfbff): MP initialization
CPU(07:000206d7 bfebfbff): MP initialization
CPU(08:000206d7 bfebfbff): MP initialization
CPU(09:000206d7 bfebfbff): MP initialization
CPU(0a:000206d7 bfebfbff): MP initialization
CPU(0b:000206d7 bfebfbff): MP initialization
Total RAM: 32768MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
```

```
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
......
Reading boot image 3712988 bytes.
Initializing FortiDDoS...\ufffd

System is started.
Updating Application Image
FortiASIC-TP.2: update started. Reconfigure process takes a few minutes
FortiASIC-TP.0: update started. Reconfigure process takes a few minutes
FortiASIC-TP.5: update started. Reconfigure process takes a few minutes
FortiASIC-TP.2: 0% Complete
FortiASIC-TP.4: 0% Complete
FortiASIC-TP.3: 0% Complete
FortiASIC-TP.5: 0% Complete
FortiASIC-TP.5: 10% Complete
FortiASIC-TP.3: 10% Complete
FortiASIC-TP.5: 20% Complete
FortiASIC-TP.4: 10% Complete
FortiASIC-TP.0: 10% Complete
FortiASIC-TP.3: 20% Complete
FortiASIC-TP.1: 10% Complete
FortiASIC-TP.5: 30% Complete
FortiASIC-TP.2: 10% Complete
FortiASIC-TP.4: 20% Complete
FortiASIC-TP.0: 20% Complete
FortiASIC-TP.3: 30% Complete
FortiASIC-TP.1: 20% Complete
FortiASIC-TP.5: 40% Complete
FortiASIC-TP.2: 20% Complete
FortiASIC-TP.4: 30% Complete
FortiASIC-TP.0: 30% Complete
FortiASIC-TP.3: 40% Complete
FortiASIC-TP.1: 30% Complete
FortiASIC-TP.5: 50% Complete
FortiASIC-TP.2: 30% Complete
FortiASIC-TP.4: 40% Complete
FortiASIC-TP.0: 40% Complete
FortiASIC-TP.3: 50% Complete
FortiASIC-TP.1: 40% Complete
FortiASIC-TP.5: 60% Complete
FortiASIC-TP.2: 40% Complete
FortiASIC-TP.4: 50% Complete
FortiASIC-TP.0: 50% Complete
FortiASIC-TP.3: 60% Complete
FortiASIC-TP.1: 50% Complete
FortiASIC-TP.5: 70% Complete
FortiASIC-TP.2: 50% Complete
FortiASIC-TP.4: 60% Complete
FortiASIC-TP.0: 60% Complete
FortiASIC-TP.3: 70% Complete
FortiASIC-TP.1: 60% Complete
FortiASIC-TP.5: 80% Complete
FortiASIC-TP.2: 60% Complete
FortiASIC-TP.4: 70% Complete
```

```
FortiASIC-TP.0: 70% Complete
FortiASIC-TP.3: 80% Complete
FortiASIC-TP.1: 70% Complete
FortiASIC-TP.5: 90% Complete
FortiASIC-TP.2: 70% Complete
FortiASIC-TP.4: 80% Complete
FortiASIC-TP.0: 80% Complete
FortiASIC-TP.1: 80% Complete
FortiASIC-TP.3: 90% Complete
FortiASIC-TP.5: FPGA image download complete.
FortiASIC-TP.5: Checking update image on FPGA.....
FortiASIC-TP.5: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.5: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.2: 80% Complete
FortiASIC-TP.4: 90% Complete
FortiASIC-TP.0: 90% Complete
FortiASIC-TP.1: 90% Complete
FortiASIC-TP.3: FPGA image download complete.
FortiASIC-TP.3: Checking update image on FPGA.....
FortiASIC-TP.3: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.3: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.2: 90% Complete
FortiASIC-TP.4: FPGA image download complete.
FortiASIC-TP.4: Checking update image on FPGA.....
FortiASIC-TP.4: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.4: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.0: FPGA image download complete.
FortiASIC-TP.0: Checking update image on FPGA.....
FortiASIC-TP.0: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.0: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.0: update finished
FortiASIC-TP.1: FPGA image download complete.
FortiASIC-TP.1: Checking update image on FPGA.....
FortiASIC-TP.1: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.1: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.1: update finished
FortiASIC-TP.2: FPGA image download complete.
FortiASIC-TP.2: Checking update image on FPGA.....
FortiASIC-TP.2: Checking update image on FPGA.....OK, GBL_RUPD_RECONFIG_
STAT = 0x3
FortiASIC-TP.2: UPDATE FPGA OK, WAIT FOR REBOOT....
FortiASIC-TP.2: update finished
FortiASIC-TP.3: update finished
FortiASIC-TP.4: update finished
FortiASIC-TP.5: update finished
FortiDDoS-1200B ( 8:27-10.26.2015)
Ver:05000002
Serial number:FI1K2B3915000007
RAM activation
CPU(00:000206d7 bfebfbff): MP initialization
CPU(01:000206d7 bfebfbff): MP initialization
CPU(02:000206d7 bfebfbff): MP initialization
```

```
CPU(03:000206d7 bfebfbff): MP initialization
CPU(04:000206d7 bfebfbff): MP initialization
CPU(05:000206d7 bfebfbff): MP initialization
CPU(06:000206d7 bfebfbff): MP initialization
CPU(07:000206d7 bfebfbff): MP initialization
CPU(08:000206d7 bfebfbff): MP initialization
CPU(09:000206d7 bfebfbff): MP initialization
CPU(0a:000206d7 bfebfbff): MP initialization
CPU(0b:000206d7 bfebfbff): MP initialization
Total RAM: 32768MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...
......
Reading boot image 3712988 bytes.
Initializing FortiDDoS...\ufffd

System is started.
FI1K2B3915000007 login:
```

Downgrading

Use the following instructions to downgrade, if necessary, from FortiDDoS 4.3.1 or earlier releases.

Note the following:

- All the configurations would be lost on downgrading using GUI, CLI or BIOS.
- **Downgrading returns the system to factory default with no user configuration. If you do not have a stored backup configuration of the earlier release and must downgrade, you will need to backup your current configuration, edit the first line to the correct destination (downgraded) firmware release, build number and date, and restore that configuration file. If you are unsure of this step, contact Fortinet Support.**
- **Downgrades below 4.1.12 are NOT recommended for bug and security reasons.** If you need to downgrade below 4.1.12 you may need to alter your current configuration, removing all NTP configurations and removing multiple remote syslog servers if configured. Please contact Fortinet Support if you need to downgrade below 4.1.12.
- When downgrading from 4.3.x to releases before 4.2.3, there may be no default IP assigned to the Management 1 port. This will need to be set via CLI. We do not recommend downgrading to releases earlier than 4.2.3.

Downgrading from 4.2.0 and earlier versions

You can use the web UI, CLI or BIOS to downgrade from 4.2.0 and later releases. You can downgrade directly to the release you want to use.

To downgrade firmware:

1. Take a backup of your configuration. Downgrade will delete the current configuration and will set everything to factory defaults.
   Use GUI:
   1. Go to **System** > **Maintenance** > **Backup & Restore** tab.
   2. Select **Back Up** option and click **Back Up**.

   or

   Use CLI:

   ```
   137-900B # execute backup config tftp 137.conf 172.30.153.105
   Connect to tftp server 172.30.153.105 ...
   Please wait...
   #
   Send config file to tftp server OK.
   ```

2. Load new build via GUI/ CLI or BIOS.
   For GUI:
   1. Go to **System** > **Maintenance** > **Backup & Restore** tab.
   2. Select the file and upload. The system will reboot.

   For CLI:

   ```
   137-900B # execute restore image tftp FDD_900B-v400-build0416-
   FORTINET.out 172.30.153.105
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)y
   Connect to tftp server 172.30.153.105 ...
   Please wait...
   ##################################################################
   ####
   ```

```
Get image from tftp server OK.
```

Verifying the integrity of the firmware image. This operation will downgrade the current firmware version! You will lose your existing configuration

```
Do you want to continue? (y/n)y
137-900B #
```

3. The system will reboot and reprogram the FPGA.
   This takes about 10-15 min based on what appliance you are using.

   WARNING: Reboot or power fail during this process will result in unusable product, requiring RMA.

4. Once the system is up, assign the IP address and restore the saved configuration. System will reboot and apply the configuration. The system should be ready to use.

Factory reset

If you want to restore a system to factory defaults with no customer configuration or traffic data, do the following from CLI:

- `# execute formatlogdisk` - removes all traffic data.
- `# execute factoryreset` - removes all configurations.

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.

Mantis ID	Description
407138	'Excessive packet per destination' floods could be reporting on incorrect SPPs.
412333	Slave HA appliance IP Gateway was being removed on reboot.
412900	Depending on release upgrade sequence, some upgrade steps were missed out, resulting in missing features. 4.3.1 will check at all required files and databases are present or create them.
413026	Simplified Chinese language GUI was not working correctly.
413886	The CLI command to reset DNS Blacklist was incorrect.
414318	FortiDDoS was not sending TC=1 Responses to suspect clients during DNS flooding.
415626	Under very heavy load conditions some thresholds could be replaced with random values.

Common Vulnerabilities and Exposures

FortiDDoS 4.3.1 is no longer vulnerable to the CVE-References in the below table.

Visit https://fortiguard.com/psirt for more information.

Mantis ID	CVE References
405140	• CVE-2017-3731 • CVE-2017-3730 • CVE-2017-3732 • CVE-2016-7055

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.

Mantis ID	Description
278685	If a user tries to enter Management IP port as Destination - 1.1.1.0/24 Gateway as 1.1.1.255 via GUI , FortiDDoS will store it as: Destination 1.1.1.0/24 Gateway as 0.0.0.0. If the user attempts to enter Gateway as 1.1.1.255 via CLI , the system returns "invalid IP address". This will only occur if the user enters an IP address ending in .255 from the GUI.
299377	If a Deny ACL is set and then removed within a five minute reporting period, the drops associated with that ACL will be shown as a 'Flood Drop Event '.
310258	System does not send RSTs to DNS server under some L7 DNS TCP floods (DNS Query/ Src, DNS Packet -Track/Src).
354467	For TCP and UDP Port graphs, if a port shows 0 traffic for a long period of time and then some traffic arrives, the port graph may show the most recent traffic across the zero-traffic period.
378756	Some 4.2.x customers are reporting that they cannot display the Event Log unless they set a filter. We have not been able to reproduce the issue but have made a change to MySQL to reduce this possibility and added debugging files in 4.3.0/4.3.1.
380993	If the alert-mail connectivity test fails, the system is unresponsive for several seconds and you cannot navigate form the page. The system/GUI will return with a failure message.
386498	Based on the hardware logic, Unsolicited Inbound DNS Responses will show in Outbound graphs.
388763	On multi-TP2 models, traffic with Ethertypes 0x9100 (QinQ) and 0x88a8 (802.1ad/aq) is not load-balanced across more than 1 TP2. Ethertype 0x8100 (802.1q) works as expected.
393803	One customer is reporting large number of drops when a Threshold is set for TCP Port 443 but there is no actual traffic on that port. We have been unable to reproduce this scenario. In normal setup and operation there are no thresholds set for TCP service ports 80 or 443 (for example) because we do not want to rate limit these ports at any time. Other meters are used to detect anomalous behavior.
397103	The default all-route IPv6 address - ::/0 - does not result in IPv6 blocking when entered in a global ACL.
397104	Some IPv6 ACL entries are not validated against previous entries for overlapping subnets.

Mantis ID	Description
397759	UPGRADES TO 4.3.1 ARE SUPPORTED FROM ANY RELEASE. However, if an attempt is made to upgrade FortiDDoS to Release 4.3.0 from any release OTHER THAN 4.2.3, the update will fail and the only recovery mechanism is to perform a factory installation via BIOS. This will result in the loss of the system configuration and all stored data for graphs and reports.
397836	While adding a large number of IPv6 ACLs from GUI, the lack of pagination support slows response times.
399196	To reduce logging, FortiDDoS attempts to combine similar small attacks before reporting in the Attack Log. If there are very large numbers of small attacks (slow connections, for example), the GUI will become slow while the background tasks are completed.
401569	Currently, system generated packets such as RSTs and SYN-ACKs/TC=1 are shown on the Port Statistics graphs but not on the SPP Statistics graphs.
402310	Under high attack loads, ICMPv6 attack events occasionally do not show the correct protected IP or subnet ID.
402435	Multiple line email messages which were allowed in previous releases are not allowed in 4.3.1.
402876	Values for SYN thresholds larger than the system maximum can be entered via CLI with no error message. Values are set to system maximum.
402886	When creating port ranges and thresholds via CLI, the system will accept an end-port number that exceeds 65535.
402907	In rare cases, if there are 100% drops for TCP Ports, UDP Ports, ICMP or URLs, Ingress traffic graphs may not show.
403850	Under heavy traffic conditions, DDoS Attack Log 'Save current page as PDF' may not create the PDF.
404070	If you are attempting to delete a large number of global addresses (IP, Subnet or Geolocation) that are used in an Access Control List, the list of addresses that is displayed may extend off the screen with the result that the OK button is not displayed.
404343	SYN ingress rates are peak rates per period while egress rates are averages over the same period, which may result in mismatched graph data.
404344	Diagnostics > Sources is showing direction as 1/0 instead of Inbound /Outbound.
404557	Entry validation of SPP IP ACLs does not check if the IP is already in a Global ACL. The global ACL takes precedence.
406382	In 4.3.1, Protection Profiles > SPP Settings > DNS Anomaly Feature Controls tab: DNS Info Anomaly does not show that Type ALL is the info anomaly enabled by this feature. Queries with type ALL/ANY will be dropped if this is enabled.

Mantis ID	Description
406872	If Persistent HTTP Transactions are disabled (default in 4.3.1) Method per Source still checks every packet for correct header. This can result in higher than expected Method counts.
409218	'Save as PDF' for Executive Summary > DDoS Attack log displays first column as 'Attack' for all tables. This is correct for some tables but incorrect for others.
411833	Report schedule hour configuration does not adjust for Daylight Savings Time change.
413459	Domain ACL list should allow 1 million entries. However, hash collisions are limiting this to about 500,000 entries. Before uploading a new list, always clear the previous list.
413613	In rare cases, after repeated upgrades and downgrades, a few graphs may stop showing on the top level Aggregate Drop page.
413659	CLI allows special characters to be used for user names but the system will not retain the special characters, resulting in an unusable user name. Do not use special characters in usernames.
413668	The "admin" user is the default user/global admin for the system. Such user should always be a local user. Currently, the authentication strategy can be changed to Radius or LDAP for user "admin".
413900	When downgrading from 4.3.x to 4.2.x, there may be no default IP assigned to the Management 1 port. This will need to be set via CLI.
415643	Downgrading the system from 4.3.x to 4.2.x or lower releases and then upgrading back to 4.3.x does not recreate eve_subcode table which will result in some attack events being missing from the logs. To prevent this, after downgrading, run `# execute formatlogdisk` before upgrading again. This step is not required if the system has never been downgraded from 4.3.x. `# execute formatlogdisk` removes all traffic data.