FortiDDoS and FortiDDoS CM 5.3.0

Release Notes

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, February 4, 2020

FortiDDoS & FortiDDoS CM 5.3.0 Release Notes

Revision 1

TABLE OF CONTENTS

Change Log

Date	Change Description
01/07/2020	Initial version of FortiDDoS 5.3.0 Release notes.

Introduction

This section provides an overview of FortiDDoS and FortiDDoS Central Manager

Introduction to FortiDDoS

Introduction to FortiDDoS Central Manager

Introduction to FortiDDoS

This document provides a list of new features and known issues for FortiDDoS 5.3.0 build 0204, including ASIC Version: 5300098 Date: Dec 4, 2019.

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

Introduction to FortiDDoS Central Manager (FortiDDoS-CM)

This document provides a list of new features and known issues for FortiDDoS-CMVM 5.3.0 build 0204

FortiDDoS-CM is designed to manage multiple FortiDDoS appliances with shared management attributes.

For specific FortiDDoS-CM information, proceed to the section - FortiDDoS-CM

For additional documentation, please visit: http://docs.fortinet.com/fortiddos

What's new

FortiDDoS 5.3.0 release includes the following new features and enhancements:

Automated Distress ACL: Distress ACL allows complex Layer 3 and Layer 4 ACLs to be configured that will block those parameters to the full bandwidth of all front panel ports, offloading the SPUs for very large attacks. Until Release 5.3.0, these ACLs were configured manually. In 5.3.0, the application of these ACLs can be automatically triggered via the SPP Switching/Signaling Threshold. Data rates higher than the signaling threshold will generate an internal list of the Top Attacks and the Layer3/4 attributes of these attacks will be configured automatically as Distress ACLs. These ACLs are monitored every 30 seconds for continued drops. When drops fall below a low threshold the ACL is retained but disabled. If later monitoring determines the ACL is required again it is re-enabled. Traffic not matching these ACLs continues to be processed by the SPUs for additional mitigation. Drops associated with the automatic Distress ACLs will be shown on the Aggregate Drop Graph, the matching Distress ACL Monitor graph and will be reported in Attack Logs.

DNS Rcode Thresholds To improve DNS Response Flood mitigation with asymmetric traffic and/or where encrypted DNS is present, Thresholds can be added as follows:

- DNS Response Code - No Error - Threshold applied to DNS R-Code 0, good Responses

- DNS Response Code - Error - Threshold applied to all DNS R-Codes from 1-15, error Responses

Note, these thresholds are not automatically learned and are not adaptive. They require manual setting by observation of the DNS R-code Monitor graphs.

Traffic and Drops for all R-codes is seen in the Monitor Graphs for DNS R-codes.

Distress ACL drop graphs are reorganized: - The aggregate of all Distress ACL drops will be shown in Monitor > Aggregate Drops

- Drops for each Distress ACL will be shown in Monitor > Distress ACL Drops

NTP Reflection Attack For E-Series only, Protection Profiles > Service Config > NTP Reflection ACL will include both NTP Monlist and Mode 6 responses.

Bypass Status on E-series Added Optical Bypass Status "LEDs" to E-Series dashboard

ACL Search User can Query system via GUI (Log & Report > Diagnostics > ACL Search) the determine if an IPv4 address is present in:

- IP Reputation

- Geo-location

- Blacklisted IPv4 Address

- Any global or SPP IP or subnet ACL

- Any Do Not Track / Track and Allow ACL

Note: This function is not available via the FortiDDoS Central Mangement GUI. You must login directly to the appliance to use it.

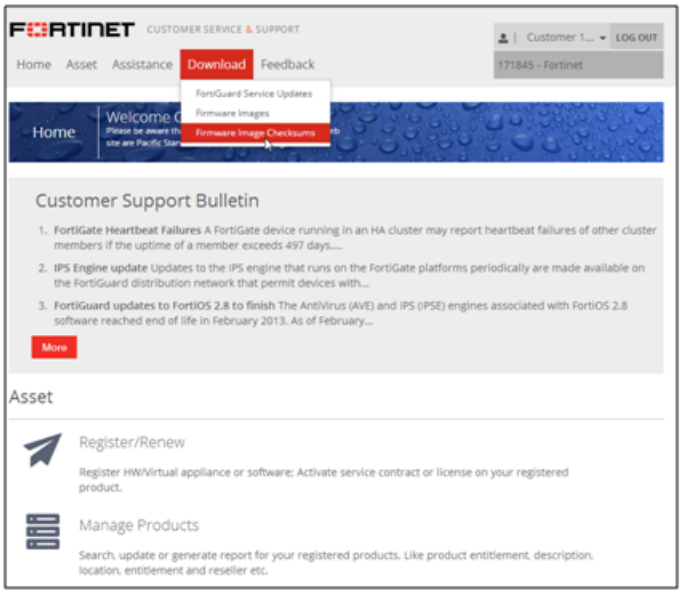
Image checksums

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

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**.

FortiDDoS

This section includes the following topics specific to FortiDDoS release 5.3.0:

For topics specific to FortiDDoS Central Manager, see FortiDDoS-CM.

Hardware support

This release supports the following hardware models:

- FortiDDoS 1500E
- FortiDDoS 2000E
- FortiDDoS 200B
- FortiDDoS 400B
- FortiDDoS 600B
- FortiDDoS 800B
- FortiDDoS 900B
- FortiDDoS 1000B
- FortiDDoS 1000B-DC
- FortiDDoS 1200B
- FortiDDoS 2000B
- FortiDDoS 2000B-USG

NOTE: FortiDDoS A series models are not supported.

Updating firmware on HA cluster

Note the following before upgrade:

- Upgrading FortiDDoS requires at least one reboot of each appliance and can be disruptive of network traffic depending on fail-open/closed conditions and RSTP/BGP settings of surrounding switches. This procedure assumes production traffic on the Master appliance with an upgrade of the Slave appliance first. This procedure can be reversed – move traffic to the Slave, upgrade the master, revert traffic and upgrade the Slave.
- If both devices are carrying production traffic (each appliance is on one leg of an asymmetric traffic environment), ensure both devices support fail-open and perform in a maintenance window.
- Do not modify any configuration settings when systems are in Standalone Mode. Any configuration changes may cause the Slave unit to reboot when returning to the HA pair.

To update the firmware of an HA cluster:

1. Verify that the cluster node members are powered on and available.
2. Log into the web UI of the Master node with an account whose access profile contains **Read** and **Write** permissions in the Maintenance and HA categories.
3. Backup the configuration.
4. Go to System > High Availability and note or take a screenshot of all settings on this page.
5. Change the HA mode from Active-Passive to Standalone.
6. Repeat steps 2-4 on the Slave system.
   Note: Having both systems in Standalone mode is important for this procedure.
7. On the Slave system, follow the upgrade procedure as instructed in the Release Note upgrading section. (This assumes that the traffic is currently on the Master system.)
8. Once the Slave system is upgraded, leave the Slave in Standalone Mode and move traffic to the Slave.
9. On the Master system, follow the upgrade procedure as instructed in the Release Note Upgrading section.
10. When upgrade of the Master system is complete, while still connected to the Master, go to System > High Availability. Confirm or set all HA settings that you retrieved from Step 4. Ensure that the Device priority is set to a higher priority (lower number) than what you have recorded for the Slave system. Then change the Master system Configured HA Mode to 'Active-Passive'.
11. Revert traffic to the Master system.
12. On the Slave appliance, go to System > High Availability. Confirm all settings from those you recorded in Step 4 and confirm or set the Device Priority to a lower priority (higher number) than the Master system. Then change Configured HA Mode to 'Active-Passive'.
13. Depending on what Release you are upgrading from, new configuration information may be available on the Master system that is not in the Slave. When the Slave sees this configuration mismatch, it will reboot in order to synchronize its configuration with the Master. This is normal and will only occur once. Once both units are synchronized, changes in the Master are synchronized to the Slave without further reboots.

Upgrading

Supported upgrade paths For B-series:

Use the following instructions to upgrade to FortiDDoS 5.3.0.

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 5.3.0. 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 5.3.0. Follow Step 3.
3	4.2.3 to 5.2.0	GUI/CLI/BIOS	1. Upgrade directly to 5.3.0. Refer to sections 1, 2 or 3 for detailed upgrade procedure.

Supported upgrade paths For E-series:

Use the following instructions to upgrade to FortiDDoS 5.3.0.

Steps	Current Release	Upgrade method	Upgrade path
1	5.0.0 to 5.2.0	GUI/CLI/BIOS	1. Upgrade directly to 5.3.0. Refer to sections 1, 2 or 3 detailed upgrade procedure.

FortiDDoS TP2/TP3 hardware 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.

To track the progress of upgrade from any version, check the console. While the back-end processes are initializing after an upgrade, a rotating GIF of several icons is displayed on the browser until the system is ready to accept login.

Clear your browser cache after upgrade to ensure new features are displayed correctly once logged-in.

Prerequisites

- The procedures explain the upgrade from 4.2.3 or higher. If your system is not at 4.2.3, refer to the table above and follow the instructions.
- Download the correct 5.3.0 firmware file for your model from the Fortinet Technical Support website: https://support.fortinet.com/.
- Check that the upgrade info file is available on your FortiDDoS system:
  - On the Dashboard page, click the CLI Console window to connect and see the command (#) prompt.
  - Enter: `f cat /var/log/upgrade_info.txt`
  - Check that the X,Y,Z number you see looks like the current Release of the system (from the Dashboard page. This file is needed to properly upgrade your system.

    Example:

    ```
    FI200B3914000071 # f cat /var/log/upgrade_info.txt
    4,7,0FI200B3914000071 #
    ```

- **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 5.3.0. 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 5.3.0.
- After upgrade you may need to regenerate system recommended Thresholds. Before upgrading, go to Protection Profiles > Thresholds > Scalars and for each SPP, use the 'Save as CSV' in the top right corner of the GUI. This will allow you to compare pre- or post-upgrade/new Recommended Threshold values.
- You must have super user permission (user admin) to upgrade firmware.

IMPORTANT:

- Releases 4.1.6, 4.1.8, 4.2.0, 4.5.0 and 4.7.0 included improvements to System Recommended Thresholds and Threshold ranges. If you upgraded from any version lower than 4.7.0, take the following additional steps after the upgrade to 5.3.0 has completed and the system has restarted:
- **If you upgraded from any Release lower than 4.2.0**: If you have DNS server(s), create a DNS SPP and SPP Policies to place the server IP(s) inside the DNS SPP. Set all DNS anomalies ON for that SPP. Leave that SPP in learning mode (no Thresholds and in Detection mode only) for as long as possible (recommended period is one week). After one week, run the Traffic Statistics and set System Recommended Thresholds. Then run for several days with Thresholds set to look for false-positives and tune if needed. Check for the volume of Anomalies. It should be a few per 5-minute reporting cycle. If there are many, remove DNS Anomalies and contact Fortinet Support.
- **If you upgraded from any Release betwen 4.2.0 and 5.0.0**: For every other SPP, about one week after the upgrade, run Traffic Statistics and set System Recommended Thresholds. This will create Thresholds that were not included in earlier Releases. Review the new Thresholds against the saved Threshold CSVs. **Note:** Review the TCP and UDP port thresholds from 1-9999. These may be higher in 5.1.0. This is design-intent. Ignore ports above 10,000. After the new System Recommended Thresholds have been set, it is recommended that the SPPs affected be placed in Detection Mode for a few days to check for false-positives and tune if needed. If in doubt, contact Fortinet Support for assistance.

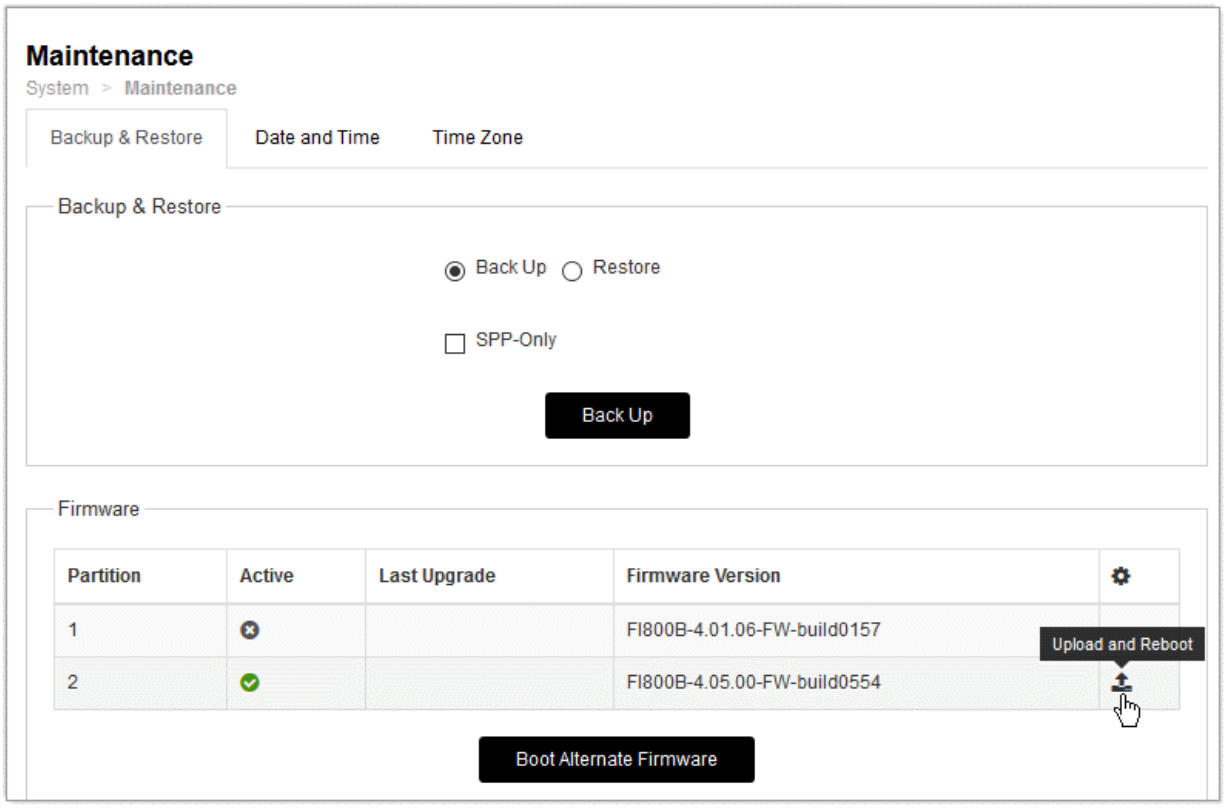
Section 1: Upgrading using GUI

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

Note: You can upgrade directly to FortiDDoS 5.3.0 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 5.3.0.

For this upgrade, you must use Partition 2. The following figure shows the user interface for managing firmware.



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 upgrade takes several (as long as 15) minutes – longer for larger systems and the system will reboot once or twice depending on the Release.** During this time, there is no progress indicator on the GUI. FortiDDoS must write register information to each TP2 which takes considerably longer than loading firmware as in most x86-based systems. This is only a factor during the upgrade. 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. It is highly recommended to connect to the Console port during an upgrade, even if using the GUI. The Console will display progress messages when the GUI is unresponsive during the upgrade.

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.

From the GUI-based Console, SSH or Console, access the command line and follow these steps:

a. Enter: `diagnose debug rrd_cmd_check`
   The console will display the percentage (%) checked messages which may scroll off the screen depending on your access method. Allow this to complete. The system will return one of the following messages on success/failure:
   - `RRD commands check successful`
     The upgrade was successful. Proceed with other actions. No further checks are required.
   - `RRD commands check failed`
     The upgrade failed to create some database. Proceed to next step.

b. Enter: `diagnose debug rrd_cmd_recreate`

c. Enter `y` when confirmation is requested.
   The Console will display the messages below, if successful:
   ```
   100% complete
   Created rrd cmd files
   ```
   If any error message occurs during this process, contact Fortinet Support. If the `100% Complete` message is seen, proceed to other actions.

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 5.3.0 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 5.3.0.

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
   - `<tftp_ipv4>` is the IP address of the TFTP server.

   For example, if the firmware image file name is `FDD_200B-v5.3.0-build0204-FORTINET.out` and the IP address of the TFTP server is 172.30.153.105, enter:

   ```
   FI900B3915000043 # execute restore image tftp FDD_200B-v5.3.0-build0204-
   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.
   ```

   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 upgrade takes several (as long as 15) minutes – longer for larger systems and the system will reboot once or twice depending on the Release**. (See the progress examples from the console output below). FortiDDoS must write register information to each TP2 which takes considerably longer than loading firmware as in most x86-based systems. This is only a factor during the upgrade. 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 run `get system status`, confirming the version information is correct:

```
Version:           FortiDDoS-200B v5.3.0,build0204,190912
TP2ASIC Version:    5300098 Date: Apr 22, 2019
IP Reputation DB:   Not enabled
Domain Reputation DB: Not enabled
Serial-Number:      FI200B3914000081
BIOS version:       04000001
Log disk:           Capacity 62 GB, Used 978 MB ( 1.52%), Free 62 GB
RRD disk:           Capacity 369 GB, Used 165 GB (44.82%), Free 203 GB
Hostname:           FDD-169
HA configured mode: active-passive
HA effective mode:  Master
Distribution:       International
License Type:       -
Uptime:             0 days  0 hours  37 minutes
Last reboot:        Thu Apr 25 15:35:18 PDT 2019
System time:        Thu Apr 25 16:25:00 PDT 2019
```

Section 3: Upgrading via BIOS

- The system configuration will be lost when upgrading via BIOS. For this reason, BIOS upgrade should only be used for:
  a. Upgrading new systems that have not been put in service.
  b. When continuity of the system configuration is not important.
- Backup your configuration before starting a BIOS upgrade. It is not recommended to attempt to restore the system configuration but it can be done by editing the configuration. This is useful only for maintaining administrative information. Please contact FortiCare TAC for further information.

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

Note: You can upgrade directly to FortiDDoS 5.3.0 via BIOS from any version.

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 # execute 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 (20:41-06.12.2018)
Ver:04000001
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...
... <---------------------------------------------- Press any key
[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]: <---------------------------- Press 'g'

Please connect TFTP server to Ethernet port "MGMT".

Enter TFTP server address [192.168.1.168]: 192.168.1.168 <---- enter TFTP server IP
Enter local address [192.168.1.188]: 192.168.1.188 <--- Enter FortiDDoS IP
Enter firmware image file name [image.out]: FDD_1000B-v5.3.0-build0204-FORTINET.out <---
    Enter Image Name
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 <------ Press
    'd'
Programming the boot device now.
.....................................................................................
.....................................................................................
..................
Reading boot image 2791231 bytes.
Initializing FortiDDoS...
System is started.
```

16. Set the management port IP address and gateway IP address using the console.
17. If you saved and edited the configuration file, restore it using the CLI or web UI.
18. If you did not save a configuration file, you must reconfigure the user accounts and system options.
19. If you have restored a configuration file, go to Protection Profiles > Factory Reset and reset every SPP in use to factory defaults (Learning Mode).
20. Treat the upgrade like a new installation with Learning mode for 1 week, creating Traffic Statistics Reports and setting System Recommended Thresholds for each SPP and so on.

Sample console log

Sample console log while upgrading from 5.0.0 to 5.3.0:

```
FI200B3914000035 # execute restore image tftp FDD_200B-v5.3.0-build0204-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.
FI200B3914000035 #
FI200B3914000081 #

The system begins to upgrade ...


Firmware upgrade in progress ...
New image: FI200B-5.3.0-FW-build0204-180612
Done. 2


The system is going down NOW !!

Please stand by while rebooting the system.
FortiDDoS-200B (20:41-06.12.2018)
Ver:04000001
Serial number:FI200B3914000081
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...
......

Reading boot image 3713003 bytes.
Initializing FortiDDoS...\ufffd



System is started.

Updating Application Image
FortiASIC-TP.0: update started. Reconfigure process takes a few minutes
FortiASIC-TP.0:   0% Complete
FortiASIC-TP.0:  10% Complete
FortiASIC-TP.0:  20% Complete
FortiASIC-TP.0:  30% Complete
FortiASIC-TP.0:  40% Complete
FortiASIC-TP.0:  50% Complete
FortiASIC-TP.0:  60% Complete
FortiASIC-TP.0:  70% Complete
FortiASIC-TP.0:  80% Complete
FortiASIC-TP.0:  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
FortiDDoS-200B (20:41-06.12.2018)
Ver:04000001
Serial number:FI200B3914000081
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...
......

Reading boot image 3713003 bytes.
Initializing FortiDDoS...\ufffd



System is started.


FI200B3914000081 login:
```

Downgrading

Use the following instructions to downgrade, if necessary, from FortiDDoS 5.3.0 or earlier releases.

Note the following:

- **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 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 5.3.0 and earlier versions

You can use the web UI, CLI or BIOS to downgrade from 5.3.0 and earlier 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-v5.3.0-build0204-
   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 may 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
520891	"Possible UDP Reflection Flood" Ports were not displayed in Exec Summary > DDoS Attack Log > Top Attacked UDP Ports
570011	Changes to System > SNMP > Config > User tab allow setting of trap receiver hosts without restricting SNMP Query users to the same hosts.
586193	Upgrading FDD-600B to Release 5.1.0 or 5.2.0 results in blocked traffic and potential network instability. Upgrade from 4.7.0 to 5.3.0.
587263	Users could change "ap-id" via CLI with unexpected results. "ap-id" is used for internal communications and should not be exposed to user modification.
589973	If formatlogdisk was used on a 5.2.0 system, the Attack Log column for SPP Operating Mode (Detection/Prevention) was removed and Event Type descriptions would no longer be displayed. If this was done, upgrade to 5.3.0 will replace the column.
592970	Drop packet capture doesn't dump packets for DNS RA Bit set anomaly
594355	In 5.2.0 only, new code in TP2 and TP3 SPUs can randomly result in a "graceful recovery" condition on an SPU. The condition is logged and shown on the Dashboard Traffic Processor Status panel. The result is a system bypass of the card (default) or a spontaneous reboot of the system to clear the processor, depending on the settings In Global Settings > Settings > Settings: Reboot On Graceful Recovery. When the SPU is in graceful recovery on FDD-200B/400B, all traffic is bypassed and no mitigation nor reporting is available. When an SPU enters graceful recovery in a multi-SPU system (all other B- and E-series models), traffic is re-balanced to other SPUs allowing mitigation to continue but at reduced throughput. Reporting is not available. Reboot may return the SPU from graceful recovery but the condition can recur very quickly or within a short time. Upgrade to 5.3.0 is the only fix to this problem.
594891	Daily Configuration Backup failed log showed status as "Success"
595704	FortiDDoS was not fully SNMPv3 compliant, including: • EngineID is encoded incorrectly resulting in some SNMP managers being unable to read it. • Handshake sequence for some variables was incorrect.
599011	Several DNS Anomalies, if enabled in SPP-0 would appear in log and graphs of all SPPs even if DNS anomalies were not enabled.

Common Vulnerabilities

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

Mantis Id	Description
602295	FortiDDoS is no longer vulnerable to CVE-2004-1653.

Known issues

This section lists the known issues in FortiDDoS 5.3.0 release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Mantis Id	Description
310258	The system does not send RSTs to DNS server under some L7 DNS TCP floods (DNS Query/Src, DNS Packet - Track/Src). Sources will be blocked if configured. It is unlikely that Source Blocking is used for DNS and also unlikely that there will be TCP-based floods which require a real connection.
354467	For TCP and UDP Port graphs, if a port shows zero 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.
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.
390662	NTP Server address string (FQDN and/or IP addresses) is not validated. Use care when entering.
397103	The default all-route IPv6 address - ::/0 - does not result in IPv6 blocking when entered in a Global ACL.
400781	During very heavy attacks the Executive Summary > DDoS Attack Log graph page may become unresponsive. So far, this has only been observed in the lab.
404557	The system allows duplicate IP addresses or IP/subnet masks between Global and SPP Address Config. Global ACLs will take precedence.
404713	In Time Zone settings under System > Maintenance, some city-pairs are not matching the correct time zone. Set the time zone based on the correct GMT offset for non-daylight-savings time.
411833	Report schedule hour configuration does not adjust for Daylight Savings Time change. For example, if reports are scheduled to run at 9:00 am, they will run at 10:00 am after time change.
413984	No HTTPS Server certificate is displayed and a certificate needs to be selected before any changes can be made on the System > Admin > Settings tab.
415244	Boot Alternate Firmware button should not be used. This option will be removed in future releases.
436137	No validation is done on IP/Domain Reputation Tunnel User name/Password entries.

Mantis Id	Description
439122	Event Remote Log allows duplicate entries. Care should be taken to avoid entering duplicates.
439530	When Global ACL list exceeds 8192 entries, the GUI may not react to additional feature settings for the ACL item.
439712	SPP ID numbers are not validated when entered via CLI. User should take care to avoid duplicates if working in CLI.
439960	When there are a very large number of connections, Diagnostic > Sessions/Sources page may not be current.
440143	SNMPv3 options are not exactly the same for Traps and Queries.
442245	Under some conditions, users with RADIUS authentication may not have access to all SPPs.
442830	If the system is in Wire Mode link synchronization and one link has failed, (resulting in second link being failed by the system) a reboot will lose that link synchronization. On reboot, the failed link will not be reflected to the second link.
443933	IP addresses added to Extended Timeout Policy are not validated against other possible entries (ACLs, SPP Policies, etc.). Add these entries with care. For example, if the same IP is entered in ACL Deny policy, and as Extended Timeout Policy, that IP will be Denied.
444070	In testing, Port Statistics and SPP Statistics graphs may not match exactly due to data collection timing. 4.4.0 and 4.5.0 release improves this and we do not think this will affect real-world information.
464136	If you delete any report while generating a large number of reports, the GUI may lose contact with the system and get locked. Reloading the page and re-login may be necessary.
467210	During system configuration restore, errors might result in partial configurations. Customer should check configuration once restored to ensure all items are restored.
469829	Changing from user-installed certificate to factory certificate may lock the GUI. Close and re-open browser to restore the GUI.
471088	A very large SPP configuration may timeout while doing an SPP Restore via GUI, resulting in a partial configuration. Check your configuration once complete and restore via CLI if this problem is experienced. This problem has not been reported from the field.
471157	If a TCP port is configured as a Global Service Port, thresholds cannot be set for that port in any SPP. This was design-intent but will be changed in a future release.
473089	If you leave pages with progress meters, while they are actively displaying progress, when you return, the progress information is lost. Examples are Factory Reset and Generate Traffic Statistics.

Mantis Id	Description
477303	If the system has both trusted hosts and RADIUS trusted hosts, the standalone trusted hosts will have precedence.
478130	Event Log entries for Domain Blacklist and Domain Reputation changes are the same and may appear to be duplicates under some conditions.
489669	If the system fails to change Slave configuration in HA setup, occasionally it will report 'Success' message. In worst case, the Slave will eventually notice a database mismatch and reboot to get the entire database.
492991	Attack Log SQL database backup will not work on Slave HA system. The system needs to be changed to Standalone, backup taken and then returned to HA mode. Attack Log **can** be saved as CSV from Slave at any time.
519240	When upgrading an HA pair, HA Group, ID and Priority are removed from the configuration on both systems.
439530 440064	When Global ACL list exceeds 8192 entries, the GUI may not react to additional feature settings for the ACL item.
531378	Rarely, under heavy traffic lab conditions, Sources may not age properly from the Source tables, resulting in Hash and/or Memory drops.
531208	On HA pairs managed by FDD-Central Manager (FDD-CM) the Slave system will reboot in certain cases after doing system a configuration restore from FDD-CM to the Master.
552139	There is one report of the Event Logs no longer showing on Log&Report > Log Access > Logs > Event tab. The system continues to generate logs but they are not displayed. The only current fix is to reboot the system.
590409	On upgrade to 5.2.0 and customer-installed SSL certificates will revert to the factory certificate but the GUI may still show the customer certificate. From GUI, select factory Certificate and Save, then select customer certificate and Save to restore the customer certificate.
608424	Drop Packet Capture is not available for DNS Response Code drops.

FortiDDoS-CM

This section includes the following topics specific to FortiDDoS-CM release 5.3.0:

For topics specific to FortiDDoS, see FortiDDoS.

Introduction to FortiDDoS-CM

FortiDDoS Central Manager (FortiDDoS-CM) VM Release 5.3.0 is available as an application running on the following virtual machine applications:

- Cirtix Hypervisor (XenServer)
- Hypervisor
- KVM
- VMware ESX/ESXi, including VSphere client, Workstation and Fusion
- Xen Open Source

FortiDDoS-CM manages both common parameters across all FortiDDoS appliances in its configuration as well as individual appliance parameters, without the need to login to each device.

FortiDDoS-CM allows you to centrally manage any number of FortiDDoS devices depending on the license type - 'Up to 10 FortiDDoS appliances' or 'Unlimited FortiDDoS appliances'.

In this release, all FortiDDoS appliances managed by FortiDDoS-CM must be the same model (FDD-1200B and FDD-2000B are treated as the same model) and use same 5.3.0 firmware. Managing groups of different models can be accomplished with separate FortiDDoS-CM configurations, which can be saved and reloaded as required to switch between groups of appliances.

This release ***does not*** support the following:

- Centralized graphical views or reporting - All graphs are viewed on the individual appliances through the FortiDDoS-CM GUI. Centralized attack reporting can be done via FortiAnalyzer and FortiSIEM.

In addition:

- While individual appliances can be set to automatically backup their configurations, only manual appliance configuration backup can be done from the FortiDDoS-CM.
- Appliance configuration restoral and firmware upgrades must be done via direct logon to the appliance.

For additional documentation, see http://docs.fortinet.com/fortiddos.

Special Notes for CM

FortiDDoS Appliances need specific SPP and SPP Policy settings to operate with FortiDDoS Central Manager. Specifically:

- All SPPs in all appliances must be identical. Some appliances my then have unused SPPs
- All SPP Policies (subnets) must be identical and assigned to the same SPPs. Some subnets may not be used in some appliances but they will appear in the SPP Policy List in all appliances.

Before attempting to configure FortiDDoS-CM with several FortiDDoS Appliances, contact Fortinet Support or your local CSE for assistance.

What's new in FortiDDoS-CM

FortiDDoS-CM 5.3.0 release includes the following new features:

FortiDDoS-CM supports all new features from FortiDDoS with the exception of Log & Report > Diagnostics > ACL Search which must be done via a direct login to each appliance.

FortiDDoS-CM supports all new features from FortiDDoS

For more details, refer to FortiDDoS-CM Online Help.

FortiDDoS-CM hardware support

This release of FortiDDoS-CM supports the following hardware models:

- FortiDDoS 200B
- FortiDDoS 400B
- FortiDDoS 800B
- FortiDDoS 1000B
- FortiDDoS 1000B-DC
- FortiDDoS 1200B
- FortiDDoS 2000B
- FortiDDoS 2000B-USG
- FortiDDoS-1500E
- FortiDDoS-2000E

NOTE: FortiDDoS A series and 600B/900B models are not supported.

Installing FortiDDoS-CM

Refer to *FortiDDoS Central Manager VM Installation Guide* here for deploying a new VM.

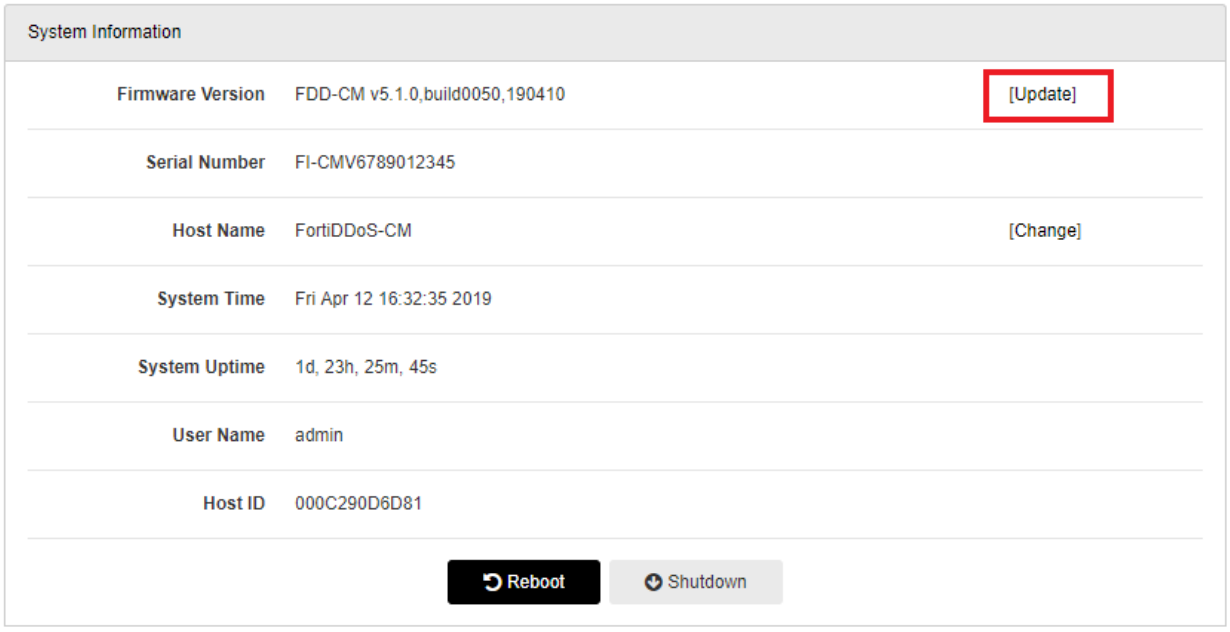
Upgrading FortiDDoS CM

Upgrading using GUI

Note: You can upgrade directly to FortiDDoS-CM 5.3.0 via GUI from any version.

To install firmware:

1. Go to CM dashboard
2. In system information widget use the Update link next to Firmware version.
3. Use the upload file controls to select the firmware image file (.out file)
4. Click **Upload** to start the firmware upgrade.
   WARNING: **While upgrading to 5.3.0 the VM may reboot twice**
5. Clear your browser cache to avoid potential issues that can be caused by caching.
   During upgrade, the VM console will show upgrade progress information.
6. Login and from **Dashboard**, confirm that the firmware version is correct.



Upgrading using CLI

Note: You can upgrade directly to FortiDDoS-CM 5.3.0 via CLI from any version.

To install firmware:

1. Login to the FortiDDoS-CM using SSH or VM console
2. Copy the image file(.out file) to a TFTP server which can be accessed from the VM's management network
3. Make sure TFTP server is running.
4. Enter the following command to transfer the firmware image to the FortiDDoS-CM system: `execute restore image tftp <filename_str> <tftp_ipv4>`

   WARNING: **While upgrading to 5.3.0 the VM may reboot twice**
5. During upgrade, the VM console will show upgrade progress information.
6. Once the system is up login and verify the firmware version using `get system status`

Downgrading FortiDDoS-CM

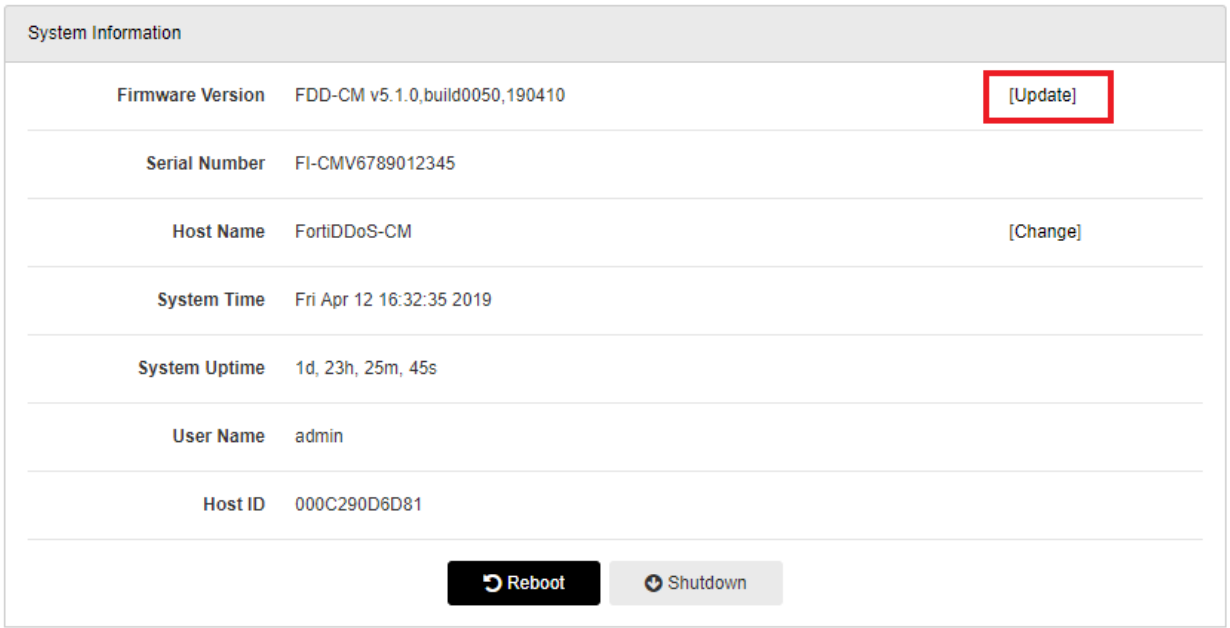
Note the following:

- **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.**
- When downgrading there may be no default IP assigned to the Port 1. This will need to be set via VM console after the downgrade is complete.

Downgrading using GUI

To downgrade using GUI:

1. Go to CM dashboard
2. In system information widget use the Update link next to Firmware version.
3. Use the upload file controls to select the firmware image file (.out file)
4. Click **Upload** to start the firmware downgrade.
5. Clear your browser cache to avoid potential issues that can be caused by caching.
   During downgrade, the VM console will show progress information.
6. Login on the console and assign the IP address, default gateway and DNS.
7. Login to the GUI and verify the firmware version under system information.



Downgrading using CLI

To downgrade using firmware:

1. Login to the FortiDDoS-CM using SSH or VM console
2. Copy the image file(.out file) to a TFTP server which can be accessed from the VM's management network
3. Make sure TFTP server is running.
4. Enter the following command to transfer the firmware image to the FortiDDoS-CM system: `execute restore image tftp <filename_str> <tftp_ipv4>`
5. During downgrade, the VM console will show progress information.
6. Login on the console and assign the IP address, default gateway and DNS.
7. Verify the firmware version using `get system status`

Resolved issues in FortiDDoS-CM

Common Vulnerabilities

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

Mantis Id	Description
602295	FortiDDoS is no longer vulnerable to CVE-2004-1653.

Known issues in FortiDDoS-CM

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
531208	On HA pairs managed by FDD-Central Manager (FDD-CM) the Slave system will reboot in certain cases after doing a system configuration restore from FDD-CM to the Master.
593464	Log& Report > Diagnostics < ACL Search is not available via the FDD Central Management GUI. You must login directly to each FortiDDoS to perform the search.

FORTINET

High Performance Network Security

Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.