

FortiDDoS and FortiDDoS CM 5.4.1

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



Friday, December 18, 2020

FortiDDoS & FortiDDoS CM 5.4.1 Release Notes

Revision 1

TABLE OF CONTENTS

| | |
|---|-----------|
| Change Log | 4 |
| Introduction | 5 |
| Introduction to FortiDDoS..... | 5 |
| Introduction to FortiDDoS Central Manager (FortiDDoS-CM)..... | 5 |
| What's new | 6 |
| Image checksums | 7 |
| FortiDDoS | 8 |
| Hardware support..... | 9 |
| Updating firmware on HA cluster..... | 10 |
| Upgrading..... | 11 |
| Section 1: Upgrading using GUI..... | 14 |
| Section 2: Upgrading via CLI..... | 16 |
| Section 3: Upgrading via BIOS..... | 18 |
| Sample console log..... | 20 |
| Downgrading..... | 23 |
| Factory reset..... | 25 |
| Resolved issues..... | 26 |
| Common Vulnerabilities..... | 27 |
| Known issues..... | 28 |
| FortiDDoS-CM | 31 |
| Introduction to FortiDDoS-CM..... | 32 |
| Special Notes for CM..... | 33 |
| What's new in FortiDDoS-CM..... | 34 |
| FortiDDoS-CM hardware support..... | 35 |
| Installing FortiDDoS-CM..... | 36 |
| Upgrading FortiDDoS CM..... | 37 |
| Downgrading FortiDDoS-CM..... | 39 |
| Resolved issues in FortiDDoS-CM..... | 41 |
| Known issues in FortiDDoS-CM..... | 42 |

Change Log

| Date | Change Description |
|------------|---|
| 2020-12-17 | Initial version of FortiDDoS 5.4.1 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 5.4.1 build 0255, including ASIC Version: 5301009a Date: August 10, 2020.

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 5.4.1 build 0255

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 5.4.1 addresses bug fixes and does not include any new features.

FortiDDoS 5.4.0 release includes the following new features and enhancements:

System Recommendations now allows separate settings for:

- Layer 4 Scalars and ICMP
- TCP Ports
- UDP Ports

System Recommendations now allows selection of:

- System Maximum Thresholds for all outbound parameters (normal enterprise deployment)
- Outbound Threshold set from Traffic Statistics (specifically for users who want outbound mitigation)

Traffic Statistics can be set to measure:

- Peak data rates for all parameters (normal for users under 10Gbps)
- 95th Percentile data rates for all parameters (used when attacks are taking place during learning)

Improvements to Automated Distress ACLs

- Remove some overly-broad ACLs
- Add more ACLs for better reflected UDP flood mitigation
- Add ACLs for "Foreign Packet" attacks

Add 25GE support on E-Series platforms

Add FEC options on 25G/40GE/100GE on E-Series platforms

Add compatibility options for syslogs:

- RFC 5424
- Support secure syslog to FortiAnalyzer over Fortinet-proprietary "OFTP"

Add REST API calls to extract Flowspec attack information

Allow creation of more than one Threshold-based Report per SPP, allowing different notifications for differing levels of attack drops.

Add CLI commands to force IP Reputation and Domain Reputation updates

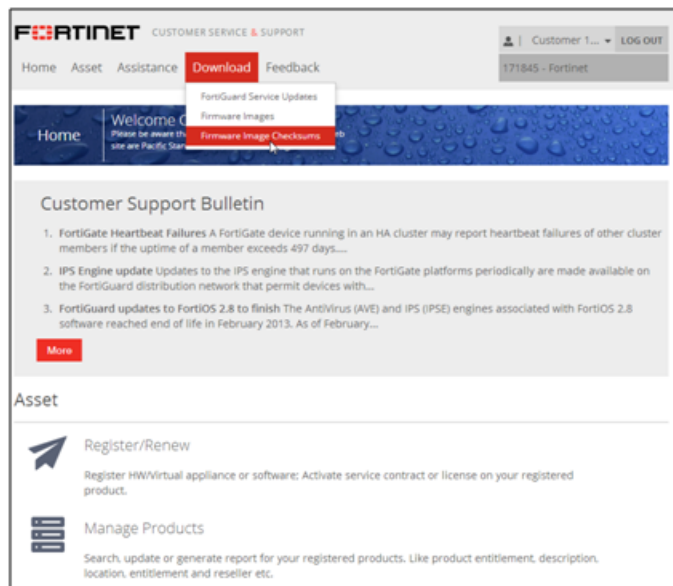
Image checksums

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 5.4.1:

Hardware support

Updating firmware on HA cluster

Upgrading

Section 1: Upgrading using GUI

Section 2: Upgrading via CLI

Section 3: Upgrading via BIOS

Sample console log

Downgrading

Factory reset

Resolved issues

Common Vulnerabilities

Known issues

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 5.4.1.

| Steps | Current Release | Upgrade method | Upgrade path |
|-------|-----------------|----------------|---|
| 1 | <4.1.5 | BIOS ONLY | <ol style="list-style-type: none"> 1. Upgrade to 4.1.5. 2. Upgrade to 4.2.3. Follow Step 2. 3. Upgrade to 5.4.1. Follow Step 3. Refer to section 3 for detailed upgrade procedure. |
| 2 | 4.1.5 to 4.2.2 | GUI/CLI/BIOS | <ol style="list-style-type: none"> 1. Upgrade to 4.2.3. 2. Upgrade to 5.4.1. Follow Step 3. |
| 3 | 4.2.3 to 5.4.0 | GUI/CLI/BIOS | <ol style="list-style-type: none"> 1. Upgrade directly to 5.4.1. 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 5.4.1.

| Steps | Current Release | Upgrade method | Upgrade path |
|-------|-----------------|----------------|---|
| 1 | 5.0.0 to 5.4.0 | GUI/CLI/BIOS | <ol style="list-style-type: none"> 1. Upgrade directly to 5.4.1. 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 5.4.1 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 5.4.1. 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 5.4.1.
- 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 5.4.1 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 between 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.

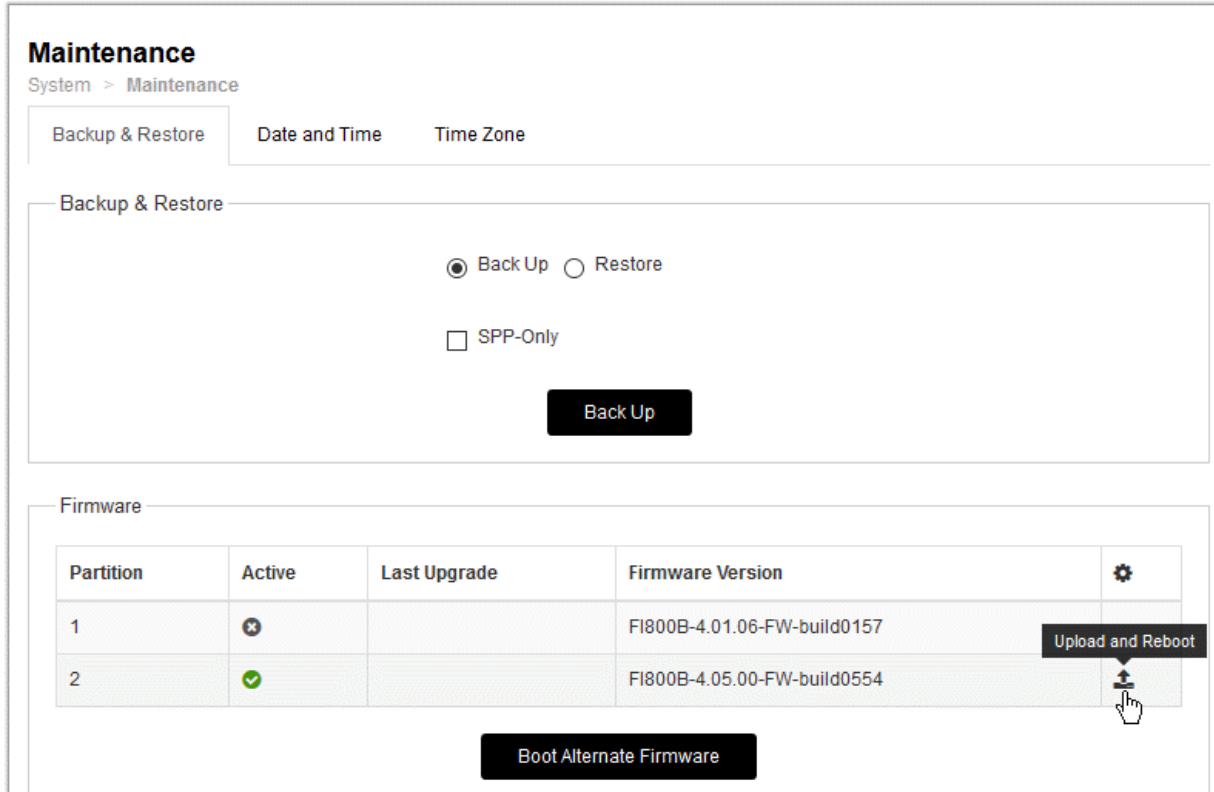
Section 1: Upgrading using GUI

Ensure that you have read the general [Upgrading](#) section before you start an upgrade.

Note: You can upgrade directly to FortiDDoS 5.4.1 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 5.4.1.

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 5.4.1 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 5.4.1.

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

For example, if the firmware image file name is `FDD_200B-v5.4.1-build0255-FORTINET.out` and the IP address of the TFTP server is `172.30.153.105`, enter:

```
FI900B3915000043 # execute restore image tftp FDD_200B-v5.4.1-build0255-
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 v5.4.1,build0255,190912
TP2ASIC Version: 5301009a 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 5.4.1 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-v5.4.1-build0255-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 5.4.1:

```
FI200B3914000035 # execute restore image tftp FDD_200B-v5.4.1-build0255-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-5.4.1-FW-build0255-180612
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 5.4.1 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 5.4.1 and earlier versions

You can use the web UI, CLI or BIOS to downgrade from 5.4.1 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-v5.4.1-build0255-
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 inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

| Mantis ID | Description |
|--------------------------|---|
| Resolved in 5.4.1 | |
| 678391 | After upgrade SPP ID1 configuration is lost |
| Resolved in 5.4.0 | |
| 489669 | Failure to sync changes from Primary HA system to Secondary showed as "success" in Event Logs. |
| 590409 | On upgrade existing SSL certificates are replaced with default |
| 600158 | Multiple "Drop Threshold" reports can be generated for any categories. |
| 612830 | The Scalar Threshold "DNS Response Code - No Error" should not be automatically created with System Recommendations. It is intended for manual application when needed. |
| 614092 | If management port IP of HA Secondary system is modified, it will revert to original IP after reboot. |
| 618282 | Ongoing developments in FortiDDoS and FOS resulted in operational instability of FortiDDoS Security Fabric integration. Please use FDD Release 5.4.1 and FOS Release 6.4.1 to ensure full availability of FortiDDoS info in FOS Security Fabric Dashboards. |
| 629490 | If a user exists on the system (with RADIUS as the authentication method) and that user attempts to login with an incorrect password, failure to reach the RADIUS server or rejection by the RADIUS server results in the user being logged-in anyway. |
| 629892 | Report Configuration, Absolute time period would only support hours 1-12. Now supports 0-23. |
| 630946 | SFTP uploads to FortiCare were not working. |
| 632885 | smtp.office365.com can now be used as the Alert Mail server with special user validation. |
| 636354 | Drop Packet capture to a single port (for example, Port 3 to capture inbound drops only) would not work if system was in Wire Mode. |
| 636721 | NTP settings ignored multiple FQDN or IP entries after the first entry. Multiple space-separated entries are now supported in order of entry. |
| 640311 | Dashboard bypass LEDs and tool tip info did not change state if CLI changed state. |

| Mantis ID | Description |
|-----------|--|
| 647012 | If system DNS settings are changed, the IP Reputation process will not use the new DNS server settings, continuing to Query the old DNS server. |
| 647175 | Formatlogdisk forces a system reboot but was not documented. Dialog box will now show warning and request confirmation (GUI or CLI) before proceeding. |
| 656074 | Qualys vulnerabilities: 1) Content-Security-Policy HTTP Security Header Not Detected - Header added 2) HTTP Public-Key-Pins Security Header Not Detected - This feature is not recommended and will be obsoleted by 2021/06 when older certificates will no longer support it. New certificates already do not support this feature. |
| 657684 | Geolocation and IP Address ACL drops were observed on E-Series in Detection Mode when neither type of ACL was enabled. These drops were removed when TP3 changes were made for other ACL (PLM) issues. |
| 660495 | Added option to disable FEC on 100GE interfaces for short-range compatibility. |

Common Vulnerabilities

For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Known issues

This section lists the known issues in FortiDDoS 5.4.1 release. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

| Mantis ID | Description |
|------------------|---|
| 670780 650221 | Due to false-positive reporting (not drops) in 5.3.0 and 5.3.1, DNS Anomalies Message Ends Prematurely, Name Too Long and Name Length Too Short have been temporarily disabled in 5.4.1. This does not increase mitigation risk. |
| 669195 | If an active IPv4 Global ACL is edited, the old ACL is retained. Do not edit Global ACLs. Delete and replace them. |
| 664402 | (E-Series only). Most Active Source drops result in miss-reporting of Most Active Source Egress traffic (increased when drops present instead of decreased). Drop information is accurate. |
| 608424 | Drop Packet Capture is not available for DNS Response Code drops. |
| 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. |
| 535380 | Failure to send Alert/Report emails is not logged. |
| 519240 | When upgrading an HA pair, HA Group, ID and Priority are removed from the configuration on both systems. Please record the HA settings before upgrading. |
| 478130 | Event Log entries for Domain Blacklist and Domain Reputation changes are the same and may appear to be duplicates under some conditions. |
| 477303 | If the system has both trusted hosts and RADIUS trusted hosts, the standalone trusted hosts will have precedence. |
| 476212 | Even though Outbound is set in Detection Mode, outbound "drops" may result in failures in TCP and DNS. Outbound settings should be reviewed to prevent drops, particularly for: - Most Active Source - SYN/Source - DNS Query Floods - NTP Query Floods |
| 473089 | If you leave Factory Reset and Generate Traffic Statistics pages, with progress meters, while they are actively displaying progress, when you return, the progress information is lost. |
| 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. |
| 469829 | Changing from user-installed certificate to factory certificate may lock GUI. Close and re-open browser restores the GUI. |

| Mantis ID | Description |
|-----------|---|
| 467210 | During system configuration restore, over slow networks, errors might result in partial configurations. Customer should check configuration once restored to ensure all items are restored. |
| 444593 | Modifying a Geolocation ACL may not modify the ACL tables. Add and delete Geolocation ACLs rather than modifying existing ACLs. |
| 442830 | If system is in Wire Mode link synchronization, and one link has failed (resulting in 2nd link being failed by the system) a reboot will lose that link synchronization. On reboot the failed link will not be reflected to the 2nd link. |
| 442245 | Under some conditions, users with RADIUS authentication may not have access to all SPPs. |
| 441880 | There is no validation between the timeouts for Slow TCP Connection Observation Period, TCP Session Idle Timeout and TCP Session Extended Timeout. Whatever period is chosen for Slow TCP Connection Observation Period, TCP Session Idle Timeout should be longer and TCP Session Extended Timeout should be longer still. |
| 439712 | SPP ID numbers are not validated when entered via CLI. User should take care to avoid duplicates if working in CLI. SPP ID numbers are automatically selected via GUI. |
| 439122 | Event Remote Log allows duplicate entries. Care should be taken to prevent entering duplicates. |
| 415244 | Boot Alternate Firmware button should not be used. This option will be removed in future releases. |
| 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. |
| 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. |
| 404557 | The system allows duplicate IP addresses or IP/subnet masks between Global and SPP Address Config. Global ACLs will take precedence. |
| 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. |
| 397104 | Some IPv6 ACL entries are not validated against previous entries for overlapping subnets. |
| 390662 | NTP Server address string (FQDN and/or IP addresses) is not validated. Use care when entering. |
| 388763 | On multi-TP2 or TP3 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. NOTE: FortiDDoS will NOT operate with QinQ traffic. |
| 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. |
| 492991 | DDoS MySQL Attack Log backup doesn't work on Slave system in HA deployment |

| Mantis ID | Description |
|------------------|---|
| 471088 | A very large SPP configuration may timeout while doing an SPP Restore via GUI on a slow network, 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. |
| 464136 | When deleting reports while also generating a large number of reports, GUI may lose contact with system and lock up. Reloading page and re-login may be necessary. |
| 444070 | In testing, Port Statistics & SPP Statistics graphs may not match exactly due to data collection timing. 4.4.0 and 4.5.0 improve this and we do not think this will affect real-world information. |
| 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 same IP is entered in ACL Deny policy, and as Extended Timeout Policy, that IP will be Denied. |
| 440064 439530 | When Global ACL list exceeds 8192 entries, the GUI may not react to additional feature settings for the ACL item. |
| 439960 | When there are a very large number of connections, Diagnostic > Sessions/Sources page may not be current. |
| 436137 | No validation is done on IP/Domain Reputation Username/Password entries. |
| 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 Attack Log will become slow while the background tasks are completed. |
| 397103 | The default all-route IPv6 address - ::/0 - does not result in IPv6 blocking when entered in a global ACL. |
| 310258 | 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. |

FortiDDoS-CM

This section includes the following topics specific to FortiDDoS-CM release 5.4.1:

[Introduction to FortiDDoS-CM](#)

[Special Notes for CM](#)

[What's new in FortiDDoS-CM](#)

[FortiDDoS-CM hardware support](#)

[Installing FortiDDoS-CM](#)

[Upgrading FortiDDoS CM](#)

[Downgrading FortiDDoS-CM](#)

[Resolved issues in FortiDDoS-CM](#)

[Known issues in FortiDDoS-CM](#)

For topics specific to FortiDDoS, see [FortiDDoS](#).

Introduction to FortiDDoS-CM

FortiDDoS Central Manager (FortiDDoS-CM) VM Release 5.4.1 is available as an application running on the following virtual machine applications:

- Citrix 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 5.4.1 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 may 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 5.4.1 release includes the following new features:

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

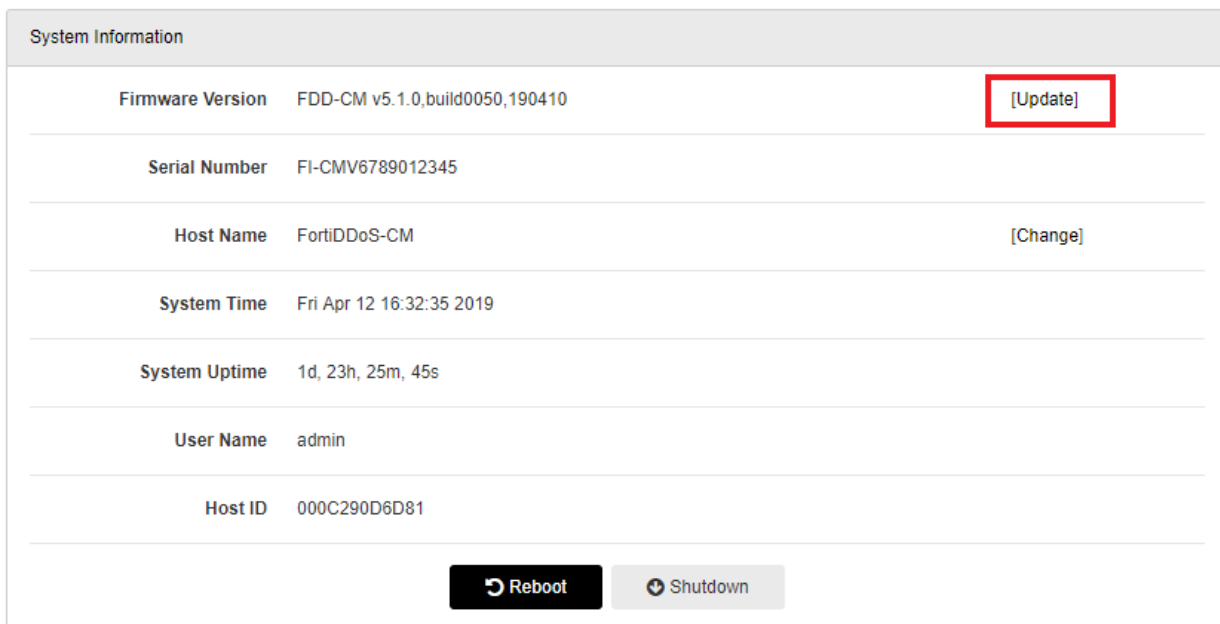
Note: You can upgrade directly to FortiDDoS-CM 5.4.1 via GUI from any version.

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.



| System Information | | |
|--------------------|--------------------------------|----------|
| Firmware Version | FDD-CM v5.1.0,build0050,190410 | [Update] |
| Serial Number | FI-CMV6789012345 | |
| Host Name | FortiDDoS-CM | [Change] |
| System Time | Fri Apr 12 16:32:35 2019 | |
| System Uptime | 1d, 23h, 25m, 45s | |
| User Name | admin | |
| Host ID | 000C290D6D81 | |

[Reboot] [Shutdown]

Upgrading using CLI

Note: You can upgrade directly to FortiDDoS-CM 5.4.1 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.

| System Information | | |
|--------------------|--------------------------------|----------|
| Firmware Version | FDD-CM v5.1.0,build0050,190410 | [Update] |
| Serial Number | FI-CMV6789012345 | |
| Host Name | FortiDDoS-CM | [Change] |
| System Time | Fri Apr 12 16:32:35 2019 | |
| System Uptime | 1d, 23h, 25m, 45s | |
| User Name | admin | |
| Host ID | 000C290D6D81 | |

[Reboot](#) [Shutdown](#)

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

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

| Mantis ID | Description |
|-----------|---|
| 613533 | NFR: FDD-CM does not allow changing SPP Detection/Prevention from SPP display in Dashboard System Status Widget |

Known issues in FortiDDoS-CM

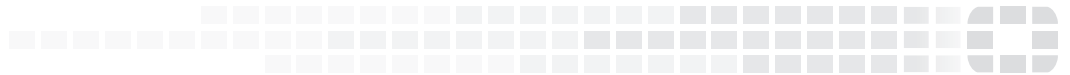
This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

| Mantis ID | Description |
|-----------|---|
| 647043 | Sync-all CM operation crashes CM if more than 6 members are out of sync. |
| 634651 | CM fails to synch more than 800 SPP Policies |
| 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.