



FortiDDoS™ 3.0 MR2

Release Notes



## FortiDDoS V3.2.0 Release Notes

May 8<sup>th</sup> 2013

Revision 1

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. 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.

Technical Documentation  
Knowledge Base  
Customer Service & Support  
Training Services  
FortiGuard  
Document Feedback

[docs.fortinet.com](http://docs.fortinet.com)  
[kb.fortinet.com](http://kb.fortinet.com)  
[support.fortinet.com](http://support.fortinet.com)  
[training.fortinet.com](http://training.fortinet.com)  
[fortiguard.com](http://fortiguard.com)  
[techdocs@fortinet.com](mailto:techdocs@fortinet.com)

# Table of Contents

- Change Log ..... 4**
- New Features..... 5**
- Upgrading ..... 6**
- Resolved Issues..... 6**
- Known Issues..... 8**

# Change Log

Date	Change Description
2013-05-08	Initial Release

# New Features

The following new features and enhancements have been added since FortiDDoS V3.1 For configuration instructions, see the FortiDDoS Administration Guide.

- Ability to Download IP Reputation data from the FortiGuard service (IRIS)
- SIP protocol Support

# System Requirements

## Upgrading

### Upgrade Procedure

FortiDDoS allow you to upgrade the firmware remotely. You will receive firmware upgrades from Fortinet, Inc. These are encrypted and encoded files. You can receive them either via email or from a File Transfer Protocol (FTP) server. Once you have this file on your workstation, you can upgrade the FortiDDoS by uploading the file to the appliance. Only administrator with the right privilege can perform this operation. Please remember that upgrades can only be reverted to one prior version .If the system requires a reboot after upgrade, you will be informed. Before upgrades, ensure that you have read these release notes and schedule the operation with your users.

To perform the upgrade, click on Manage > Global > Device Configuration > Upgrade Device.

- You will see Upgrade History as a list. This shows you past upgrades that were performed on this appliance.
- In the Upgrade section of the screen, click on Browse button and point to the file that you have received from Fortinet, Inc.
- Click on Upgrade button.
- If for some reason, the upgrade cannot be performed, the appliance reverts back to the prior version.
- If for some reason, you want to revert to the prior version click the Revert to Previous Version button. System determines if such an operation is permissible. If the operation is not permissible, this button is disabled

## 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 [Customer Support](#).

Table 1: Resolved issues.

Bug Reference	Description
0193235	Session diagnostics - Top Servers did not display any entries...
0193231	Top URL Hash Indexes shown is capped to 512 max
0185259	URL Flood Events Graphs were not shown

0192662	GET Opcode graph - show with estimated threshold did not work
0200298	HTTP Mandatory Header multiple config issue in User Interface caused header violation threshold to go back to default value
0201202	List of events shown in Reports – is now descending order based on packet drop count
0198258	Added boundary limit value - 511 for HTTP UA/Host/Refer/Cookie did not show up in Blocking threshold
0198275	CLI - show httpmeter cookie/Host/Refer/UserAgent debug - gave error - Debug Register File Not Found?
0197176	Session diagnostics - Top HTTP URLs URL name was not displayed
0192200	HTTP GET Opcode flood led to Source Flood events
0193838	Traffic Statistics - Top URL Hash Indexes showed wrong URL
0197101	Could not change timezone
0198112	Layer 7 My list had no validation
0202734	L7 Headers – did not show stats in Session Diagnostics for card 2/3
0202733	L7 headers - deny bit was not getting set for all cards
0194675	URL flood doesn't update max packet rate graph, and showed a spike after URL flood stops
0193946	STM was not blocking correctly when there is high Random source Traffic
0193385	Source Tracking Penalty Factor for URL Flood Penalty was not setting correct value in the CLI.
0194519	PUT Opcode packets were shown with no traffic
0193825	Old events were appearing with delay along with the new events
0194528	Graceful Hardware Recovery triggered with stress test
0200346	Event notification - Syslog feature was not working
0200127	SNMP traps are not received at the registered trap receiver

# Known Issues

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

Table 2: Known issues.

Bug ID	Description
N/A	Web Browsers will report error due to caching and cache will need to be refreshed
0197895	HTTP URL/ICMP Type-Code graph doesn't go back to zero once traffic is stopped
0200315	Excessive concurrent connections/dest appears in random VIDs where there is no traffic
0200982	Excessive concurrent conn/src doesn't show up in TOP ATTACKS if it's set as "Block new TCP Conn request"
0201532	Reports: traffic stats doesn't show any packets for Register/Src
0202045	Global factory default is not resetting the deny/allow source configuration
0202352	Subnet Reports shows only the last SPP IP Address if subnet id is same
0202750	Syn packet count is not correct in traffic statistics
0202711	Enabling /disabling proxy IP/ IP Reputation is causing SYN flood from source drop