



FortiTester - Release Notes

Version 7.2.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

January 13, 2023

FortiTester 7.2.1 Release Notes

00-721-872327-20230113

Change Log

Date	Change Description
January 13, 2023	Initial release.

Introduction

FortiTester™ appliances offer enterprises and service providers a cost-effective solution for performance testing and validating their network security infrastructure and services, providing a comprehensive range of application test cases to evaluate equipment and right-size infrastructure. All test functionality is included in one simple device-based license.

FortiTester provides powerful yet easy-to-use test cases that simulate many stateful applications and malicious traffic. Built-in reporting provides comprehensive information about the tests, including SNMP stats from the device under test (DUT). It enables you to establish performance standards and conduct audits to validate that they continue to be met. A single 40-GE appliance allows over 20 million concurrent connections and new HTTP connection rates greater than 1 million/second; hardware-based acceleration supports new HTTPS connection rates above 20,000/second. Up to 8 appliances can be grouped in Test Center mode to massively scale performance. 40-GE device interfaces can be split to 4x 10-GE SFP+ for additional testing flexibility. 100- and 10-GE devices and their VM versions complete the Tester range, offering competitive price points for their target customers.

FortiTester implements DPDK, which provides libraries and user-space NIC drivers for accelerated packet processing performance. The implementation allows FortiTester to offer comprehensive line-rate testing on server-class hardware.

The *Release Notes* cover the new features, enhancements, known and resolved issues, and upgrade instructions about FortiTester Version 7.2.1, Build 0351.

For additional documentation, please visit: <http://docs.fortinet.com/fortitester>.

What's new

FortiTester 7.2.1 offers the following new features and enhancements:

Function enhancement

FortiTester 7.2.1 extends the maximum number of subnets to 16.

Subnet

IP Address or Range

17.1.2.2-17.1.2.201

Netmask

16

VLAN ID

1

☐

Range: 1 - 4,094

IP Address or Range

17.2.2.2-17.2.2.201

Netmask

16

VLAN ID

1

☐

Range: 1 - 4,094

+

Subnet

IP Address or Range

17.1.1.100

Netmask

16

VLAN ID

1

☐

Range: 1 - 4,094

IP Address or Range

17.2.1.100

Netmask

16

VLAN ID

1

☐

Range: 1 - 4,094

+

FortiTester 7.2.1 extends the maximum number of configurations in an iMIX object to 20.

+ Create New

Edit

Delete

Search

No.	Packet Size	Frame Size	Percentage	Weight
1	59	77	9.52%	2
2	70	88	4.76%	1
3	69	87	4.76%	1
4	79	97	4.76%	1
5	74	92	4.76%	1
6	81	99	4.76%	1
7	76	94	4.76%	1
8	77	95	4.76%	1
9	80	98	4.76%	1
10	72	90	4.76%	1
11	58	76	4.76%	1
12	56	74	4.76%	1
13	54	72	4.76%	1
14	51	69	4.76%	1
15	50	68	4.76%	1
16	48	66	4.76%	1
17	1006	1024	4.76%	1
18	238	256	4.76%	1
19	110	128	4.76%	1
20	46	64	4.8%	1

FortiTester 7.2.1 will show two new columns for statistics, which is "Send PPS" and "Receive PPS"

port1-port2

Q Search

Direction	Frame Bytes	Cycle ID	Traffic Flow	Send Packets	Receive Packets	Send Mbps	Receive Mbps	Send PPS	Receive PPS	Loss Rate	Trial Second	Time
Unidirection...	83	1	Client -> Server	128,226	128,226	3.52	3.52	4,274	4,274	0%	30.000000	2022-12-01 15:14:16
Unidirection...	82	1	Client -> Server	768,754	768,754	20.91	20.91	25,625	25,625	0%	30.000000	2022-12-01 15:14:16
Unidirection...	81	1	Client -> Server	128,226	128,226	3.45	3.45	4,274	4,274	0%	30.000000	2022-12-01 15:14:16
Unidirection...	80	1	Client -> Server	128,226	128,226	3.42	3.42	4,274	4,274	0%	30.000000	2022-12-01 15:14:16
Unidirection...	79	1	Client -> Server	128,226	128,226	3.39	3.39	4,274	4,274	0%	30.000000	2022-12-01 15:14:16
Unidirection...	78	1	Client -> Server	128,226	128,226	3.35	3.35	4,274	4,274	0%	30.000000	2022-12-01 15:14:16
Unidirection...	77	1	Client -> Server	128,226	128,226	3.32	3.32	4,274	4,274	0%	30.000000	2022-12-01 15:14:16
Unidirection...	76	1	Client -> Server	1,281,056	1,281,056	32.80	32.80	42,701	42,701	0%	30.000000	2022-12-01 15:14:16
Unidirection...	75	1	Client -> Server	128,226	128,226	3.25	3.25	4,274	4,274	0%	30.000000	2022-12-01 15:14:16

iMIX BPS to FPS

FortiTester can perform iMIX testing. Pre 7.2.1 calculation of packet distribution was done based on "weight" variable in GUI, FortiTester used weight to calculate bandwidth per second (BPS). in 7.2.1 FortiTester introduce a new way to test using frames per second (FPS). Note this is more inline with Breaking Point distribution, hence it's the default. Users can switch back to BPS if necessary using CLI. For details between BPS and FPS, please refer to administration guide.

The command is `diagnose weighttype setting disable/enable`.

Disable: Weight type of iMIX object takes as FPS.

Enable: Weight type of iMIX object takes as BPS.

```
FortiTester # diagnose
config      Diagnose upgrade configuration.
fds         Connect fds facility.
gui         Enable/disable gui upload.
hardware    Hardware info.
sys         Diagnose system.
vmlicense   vmlicense.
weighttype  Configure weight type for iMIX object. The default disabled is flow. Enable is bandwidth.

FortiTester # diagnose weighttype setting
disable     Disable.
enable      Enable.
```

Hardware support

This release supports the following hardware models:

- FortiTester 100F
- FortiTester 2000D
- FortiTester 2000E
- FortiTester 2500E
- FortiTester 3000E
- FortiTester 4000E
- FortiTester VM (VMware ESX/ESXi, KVM, OpenStack, AWS, AZURE, GCP, OCI, ALI, and IBM Cloud)

Upgrade/downgrade instructions

You can use FortiTester's web UI to upgrade the firmware image.

Before you begin:

- Back up your configuration (From the GUI, click **System > Reset/Backup/Restore > Backup**).
- Record the current version your system is running before upgrade. This can be found in **GUI > Dashboard**, or from CLI "get system status".
- Download the image file from the Fortinet support website.
- Read the *Release Notes* for the version you plan to install.
- Upgrade the firmware from the System page.

Note: If you are using the Test Center feature, Test Center Clients will be disconnected during the upgrade, and must be reconnected after the upgrade is completed.

To upgrade the firmware:

Note that CLI is the only way to upgrade FortiTester-2000D from any pre-2.7.0 version. The Web UI does not support this upgrade. Connect to the CLI through a terminal emulator such as Putty using the following steps:

1. Start a terminal emulation program on the management computer, select the COM port, and set the baud rate as 9600.
2. Press Enter on your keyboard to connect to the CLI.
3. Login with the username - **admin** and its password.
4. Reboot the system using command `execute reboot`.
5. Select **F** to format the boot device.
6. Select **G** to download the image from the TFTP server mentioned in "Before you begin". You will be required to specify IP addresses of the TFTP server and the FortiTester appliance (management port). Make sure that both of the IP addresses are in the same subnet.
7. Select **D** to save the image file as "Default firmware" for upgrading.
8. System starts rebooting. During the rebooting process, the system will take 2~3 minutes to replace the firmware on the active partition (the message "Reading boot image ... bytes." appears). Please be patient while the system is rebooting.
9. After reboot, IP address of the management port is set to a default of 192.168.1.99. It can be changed through the following commands:

```
FAD15D3114000001 # config system interface
FAD15D3114000001 (interface) # edit mgmt
FAD15D3114000001 (mgmt) # set ip <IP_Address> <Netmask>
FAD15D3114000001 (mgmt) # end
FAD15D3114000001 #
```
10. Firmware upgrade is completed. Access the Web UI through the management port. You might need to refresh the Web UI pages by pressing **Ctrl+F5**.



FortiTester v7.2.1 does not support downgrading to previous releases. Users have the option of backup configuration and tests cases before upgrading, or restoring older firmware and configuration if necessary.

Note: If the user wants to upgrade to 7.2.1, it's best to come from version 7.0.0. Users with versions before 7.0.0 should first upgrade to 4.x then to 7.0.0, before upgrading to 7.1.0

Accelerator cards

All hardware models of FortiTester except 100F and 2000E have a performance-enhancing SSL acceleration. This helps accelerate SSL traffic in the handshake stage.

To check which card and card model your device uses:

Enter the following CLI command:

```
diagnose hardware info
```

The following information will be displayed:

```
...  
[Accelerator info]  
SSL Accelerator Model<Model number>
```

Model III represents the Cavium Nitrox III card, model V represents the Cavium Nitrox V card, and model VI represents the Intel QAT card.

Resolved issues

The following table lists the major issues that have been resolved in this release. 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 at <https://support.fortinet.com>.

Bug ID	Description
815376	The performance of some cases being lower than in version 7.1.0 is fixed
864461	IPsec Remote Access CC throughput shows up to 4G
838073	The "No memory to create mbuf for simuser " error when running UDP test with DNAT enabled on AliCloud is fixed
860914	Upgraded Pillow libraries
856577	Upgraded CURL libraries
792118	Upgraded openssl libraries
858170	Upgraded net-snmp libraries
858997	No error message shows up when file 'conf.yml' is missing

Known issues

The following table lists the major issues that are known in this release. For inquiries about a particular bug, please contact Fortinet Customer Service & Support at <https://support.fortinet.com>.

Bug ID	Description
758945	Cannot run/create case if TC_Client connects to TC_Server by Public IP
751949	EMIX throughput using Fortinet EMIX Traffic template gives lower results compared to Ixia /BP EMIX Traffic profile
738156	FortiTester agent is not digitally signed and is detected by FortiEDR as a suspicious file
697147	FortiTester SSL/VPN test does not reflect the FortiClient connections
705388	Test import fails if the test exists in another work mode or fanout mode

Change Log

Date	Change Description
January 13, 2023	Initial release.



Copyright© 2023 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.