

FortiTester Release Notes

VERSION 4.1.0

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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



November 23, 2020

FortiTester 4.1.0 Release Notes

Change Log

Date	Change Description
November 23, 2020	FortiTester 4.1.0 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 4 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.

This *Release Notes* covers the new features, enhancements, known and resolved issues, and upgrade instructions about FortiTester Version 4.1.0, Build 0018.

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

What's new

FortiTester 4.1.0 offers the following new features and enhancements:

Performance/Traffic testing

Application mode for SLL-VPN CPS/RPS/CC/Throughput cases

Added empty tunnel mode for SSL-VPN CPS case

Systems

Improved diagnose fds connect CLI command

Now FortiTester can get logs of verification for its FDS (FortiGuard Distribution Systems) license and service.

New platform support

FortiTester 4.1 release supports a new low end platform FTS-100F.

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, and OCI)

Upgrade 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**).
- 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 Slaves 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**.

Accelerator cards

All hardware models of FortiTester except 100F and 2000E have a performance-enhancing SSL acceleration, such as SSL handshake.

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
666793	All cases cannot run if FTS receives ARP reply packets vlan PRI or CIF, but not all packets are 0.
673858	The widget scroll bar should be able to be fixed to a specific position.
673861	Frag type data is not sent in the configured proportion.
674217	FortiTester proxy mode, the traffic FortiTester server side sent won't pass DUT, if DUT has enabled NAT.
675464	Failed to create a new SSLVPNCPs NAT case.
673866	Missing IP validation of networking configure in Proxy Mode.
673879	Can create web crawler network object with IP range but cannot refer this network object in case.
673296	Http_Attempted does not fill all VPN-CC tunnels in every period of think time.
671017	Case configuration misses some attributes when the case is created by API.
672621	Start case fails when test case uses the certificate with Passphrase.
671963	All maximum Concurrent Connections default values are incorrect.
671020	Statistics data of VPN is not correct.
671336	FortiTester Does not send ARP request packet of gateway IP in Proxy VR mode.
629411	FortiTester SSL VPN CC "Layer2 Bandwidth" is the same with different payload sizes.

Known issues

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

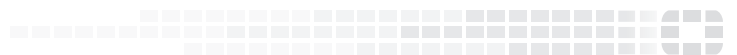
Bug ID	Description
661617	The SMB protocol performance value measured by FortiTester is different from the windows client.
674595	Frame size in load setting & MTU size in network setting should not include VLAN 4Bytes header size.
672304	FortiTester report generation is slow

Change Log

Date	Change Description
November 23, 2020	FortiTester 4.1.0 initial release.



FORTINET®



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.