FortiTester Release Notes

VERSION 4.1.1

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/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

January 4, 2021
FortiTester 4.1.1 Release Notes

Change Log

Date	Change Description
January 4, 2021	FortiTester 4.1.1 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 malicous 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 4.1.1, Build 0026.

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

What’s new

FortiTester 4.1.1 offers the following new features and enhancements:

Three new TCP options

1. TCP Window Scale

This value will allow the TCP connection to negotiate the window scale option as per RFC1323. The value set can be from 0-14 with 0 being disabled. The value set will be the maximum window size that the connection will attempt to negotiate. The window scale factor is the number of bits by which to shift the window size.

All cases based on TCP are supported. The default value is 0 (disable scale).

2. Ack every N

In order to reduce the network bandwidth occupied by the TCP header, FortiTester dynamically adjusts delay ACK time. This value will force the sending of an ACK at least every N TCP segments. Since this option is a form of delayed acknowledgment, it only works when 'Delayed Acks' is enabled.

Forcibly changing the ACK sending pattern is not RFC compliant and can result in unexpected behavior. The TCP protocol itself limits the flexibility of the 'ACK every N' mechanism. In some scenarios we must send an ACK no matter what; this implies that we might send some ACKs earlier that some would expect if the receiver's window fills, the flow ends or the TCP burst ends.

3. Initial Congestion Window

Determines the size of the initial congestion window.

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, and ALI)

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. 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 inquires about a particular bug, please contact Fortinet Customer Service & Support at https://support.fortinet.com.

Bug ID	Description
0684368	FortiTester test check echo reply packet has an incorrect icmp checksum, causing failure on NP7 tests.
0661953	Low performance when testing VPN SSL test cases CPS / RPS / TP.
0661617	The SMB protocol performance value measured by FortiTester is different from the windows client.

Known issues

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

Bug ID	Description
0674595	Frame size in load setting and MTU size in network setting should not include VLAN 4Bytes header size.
0672304	FTS report generation is slow.
0681075	API endpoint for network config object returns multiple versions of object.
0684089	Can't backup case configuration and case results.

Change Log

Date	Change Description
January 4, 2021	FortiTester 4.1.1 initial release.