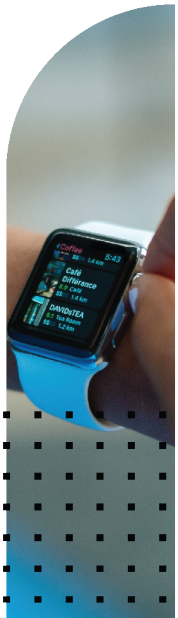
Release Notes

FortiTester 7.2.2



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

March 22, 2023
FortiTester 7.2.2 Release Notes
64-722-884560-20230322

TABLE OF CONTENTS

Change log

Date	Change description
March 22, 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 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 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 7.2.2, Build 0359.

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

What's new

FortiTester 7.2.2 is a patch release and no new features and enhancements are covered in this release.

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.

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:

```
FortiTester # config system interface
FortiTester (interface) # edit mgmt
FortiTester (mgmt) # set ip <IP_Address> <Netmask>
FortiTester (mgmt) # end
FortiTester #
```

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 7.2.2 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.

To upgrade to 7.2.2, 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 inquires about a particular bug, please contact Fortinet Customer Service & Support at https://support.fortinet.com.

Bug ID	Description
864461	IPsec Remote Access CC throughput is stuck at 1.2G. The same test on Remote Access shows up to 4G.
871018	FortiGate CPS performance under the VLAN interface is 60% worse than the physical interface.
872714	Injected a "host" header.
872791	Upgraded CURL libraries.
883246	There is an issue in handling the http response with either content-length or chunk encoding methods.
883785	FortiTester 7.2.1 GUI Online Help opens up to the 4.2 Handbook help page.
888236	There is a "fdsProxyPort str type expected" error message when the "Explicit Proxy for FortiGuard server" IP address is modified.

Known issues

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

Bug ID	Description
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.
751949	EMIX throughput using Fortinet EMIX Traffic template gives lower results compared to Ixia /BP EMIX Traffic profile.
758945	Cannot run or create case if TC_Client connects to the TC_Sever by a Public IP.

www.fortinet.com