FortiSandbox Cloud - Release Notes

Version 22.2

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

June 28, 2022
FortiSandbox Cloud 22.2 Release Notes
34-222-807482-20220628

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Upgrade Information **6**
Upgrade link not visible 6
Before and after any firmware upgrade 6
Upgrade path 6
Upgrade procedure 6
Downgrading to previous firmware versions 7
New features and enhancements **8**
CLI 8
GUI 8
Fabric integration 8
Scan 8
System & Security 9
Logging & Reporting 9
Product Integration and Support **10**

Change Log

Date	Change Description
2022-05-17	Initial release.
2022-06-28	Updated New features and enhancements on page 8

Introduction

This guide provides release information for FortiSandbox Cloud version 22.2 build 4134.

For information on deploying and maintaining FortiSandbox Cloud, see the *FortiSandbox Cloud 22.2 VM Install Guide*.

FortiSandbox Cloud build 4134 is based on FortiSandbox 4.2.0 build 0192. For the FortiSandbox features, refer to the *FortiSandbox 4.0.0 Release Notes*.

Upgrade Information

Upgrade link not visible

If you are upgrading from beta build 4105 and the upgrade link on the Dashboard is not visible, you can only upgrade by going directly to the following URL on your browser:

https://<account-id>.<region>.fortisandboxcloud.com/fortisandbox/about/sysupgrade

Before and after any firmware upgrade

Before any firmware upgrade, save a copy of your FortiSandbox Cloud configuration by going to *Dashboard* > *System Configuration* > *Backup*.

After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox Cloud so that web UI screens display properly.

Upgrade path

FortiSandbox Cloud 22.2 officially supports the following upgrade path.

Upgrade from	Upgrade to
22.1 Build 4113	22.2 Build 4134

Upgrade procedure

You can manually upgrade the FortiSandbox Cloud firmware, or download and upgrade the recommended or available builds.

To manually update the firmware:

1. Download the firmware image from the Fortinet Customer Service & Support portal.
2. Go to *System* > *Dashboard* . In the *System Information* widget, click the*View all firmware* icon next to *Firmware Version*. The *FortiSandbox Firmware Information* page opens.
3. Under *Upload Firmware*, click *Upload Firmware*.
4. Click *Upload File* and *browse* to the firmware image on your computer and click *Submit*.

5. Microsoft Windows Sandbox VMs must be activated against the Microsoft activation server if they have not been already. This is done automatically after a system reboot. To ensure the activation is successful, port3 of the system must be able to access the Internet and the DNS servers should be able to resolve the Microsoft activation servers.

Downgrading to previous firmware versions

Downgrading to previous firmware versions is not supported.

New features and enhancements

The following is a list of new features and enhancements in version 22.2.

CLI

- Enhanced `device-authorization` to enable/disable inline-block on FortiGate.
- Enhanced `test-network` to check FortiAnalyzer, Cloud VM, and Public Cloud internal connectivity.
- Enhanced `show` command to list the HC external IP.
- Updated `tac-report` relating to new features on this release.
- Added `device-clean-pdf` to enable/disable FortiSandbox Cloud to generate PDF report for clean rating jobs when requested by device.

GUI

- Introduced *Scan Performance* page for tracking historical usages.
- Upgraded GUI framework to Neutrino.
- Added FortiAnalyzer on the *Connectivity* widget.
- Added FortiNDR on the *Connectivity* widget.
- Added *Last 7 days* option to *System Resources Usage* widget.
- Added recorded video link on *Job Detail* page.

Fabric integration

- Introduced Inline Blocking feature with FortiGate FortiOS 7.2.
- Added configuration of aggregate interface via JSON RPC.
- Added option to download Macro content via JSON RPC.
- Re-introduced FortiAI as FortiNDR with new network response detection features.
- Supported FP/FN marking via JSON RPC including auto submission to Fortinet.
- Supported system resource check via API.

Scan

- Introduced *Pipeline Scan Mode* for reducing VM maintenance overhead.
- Introduced *Rating Engine Service* mode to improve performance.
- Enhanced log tracking on *Dynamic Analysis* for resiliency.

- Improved handling of similar URL when its payload has changed.
- Adjusted *Dynamic Scan* timeout value with a minimum of 30 seconds on high-end models.

System & Security

- Supported backup, restore and revision of the configuration.
- Upgraded OpenSSL library.

Logging & Reporting

- Introduced customizable reports for white-labelling.
- Added *Submit Time*, *Rated By* and *File Type* fields on the FortiAnalyzer logs.
- Enhanced naming results shown on *Rated By* of the job reports.
- Send periodic log of *Scan Statistics* to FortiAnalyzer.
- Send periodic log of *System Resource* usages to FortiAnalyzer.

Product Integration and Support

The following table lists FortiSandbox Cloud version 22.2 product integration and support information.

Web browsers	• Microsoft Edge version 99 • Mozilla Firefox version 98 • Google Chrome version 98 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 7.2.0 • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later
FortiAnalyzer	• 7.2.0 • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later
FortiManager	• 7.2.0 • 7.0.0 and later • 6.4.0 and later • 6.2.1 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later
FortiMail	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.4.0 and later
FortiClient	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiEMS	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later

	• 6.0.5 and later
FortiADC	• 7.0.0 and later • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later • 5.4.0 and later • 5.3.0 and later • 5.0.1 and later
FortiProxy	• 7.0.0 and later • 2.0.0 and later • 1.2.3 and later
FortiWeb	• 7.0.0 • 6.4.0 and later • 6.3.5 and later • 6.3.2 and later • 6.2.0 and later • 6.0.0 and later • 5.8.0 and later • 5.6.0 and later
AV engine	• 00006.00266
System tool	• 04002.00019
Traffic sniffer	• 00005.00239
Virtualization environment	• VMware ESXi: 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.1. • KVM: Linux version 4.15.0 qemu-img v2.5.0 • Microsoft Hyper-V: Windows server 2016 and 2019

Copyright© 2022 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.