FORTINET

Release Notes

FortiSandbox 4.2.1

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

April 12, 2023
FortiSandbox 4.2.1 Release Notes
34-421-802567-20230412

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-08-02	Initial release.
2022-08-08	Added Special Notices on page 8.
2022-08-26	Add Product Integration and Support on page 13.
2022-09-29	Updated New features and enhancements on page 6.
2022-10-18	Updated Resolved Issues on page 15.
2023-03-22	Updated Known Issues on page 17.
2023-04-12	Updated Resolved Issues on page 15.

Introduction

This document provides the following information for FortiSandbox version 4.2.1 build 0229.

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 4.2.1 Administration Guide* and *FortiSandbox 4.2.1 VM Install Guide*.

Supported models

FortiSandbox	FSA-3000F, FSA-3000E, FSA-2000E, FSA-1000F-DC, FSA-1000F, and FSA-500F
FortiSandbox-VM	AWS, Azure, Hyper-V, KVM, and VMware ESXi

This version no longer supports FSA-1000D, FSA-3000D, FSA-3500D, and VM Base as of version 4.0.0.

New features and enhancements

The following is summary of new features and enhancements in version 4.2.1. For details, see the *FortiSandbox4.2.1 Administration Guide* in the Fortinet Document Library.

GUI

- Added Notice on the *Community Cloud* icon of the *Connectivity and Services* widget when community submission is disabled.
- Enhanced tooltip message on update icon for the *VM Clone* on *VM Settings* page.
- Simplified license upload to a single link on hardware unit.
- Supported French translation on labels and messages related to new features.
- Supported Japanese translation on labels and messages related to new features.
- Supported *Trusted Host* on administrative GUI login of up to 50 entries.

Fabric integration

- Introduced network share scanning on Microsoft Azure Blob Storage.
- Allowed device registration even if no VMs configured yet.
- Added JSON API to support configuration of *VM Scan* timeout for non-executable file.

Scan

- Introduced Windows Cloud VM Service on appliance-based for expansion of VMs.
- Re-introduced *Upload detection statistics to FortiGuard* to upload both summary and detailed info.
- Enhanced caching of results for *Inline Block*.
- Enhanced scan engine to improve fault tolerance.
- Enhanced scan logic for Inline Block to handle duplicate submissions.
- Enhanced scan logic to detect BSOD on Windows.
- Supported *Not Applied* and *Unknown* option on *Customized Rating* for the timeout and encrypted settings.
- Supported cloud query for known FortiGuard Allowlist/Blocklist websites.

System & Security

- Improved licensing logic on additional licenses.
- Supported Office2019 upgrade license.
- Supported FSA-VM00 as dispatcher mode.

Logging & Reporting

- Supported exclusion of clean behavior on *Job Report* to reduce content and easily identify suspicious behavior.
- Supported FQDN on Log Server configuration.
- Added *http_host* and *session_id* information of *FortiWeb* on *Job Report*.
- Added message ID field of MTA Adapter deployment on *Job Report*.
- Added Web browser information on *Job Report*.

Special Notices

Upgrade path

A feature that was introduced in FortiSandbox v4.2.0 causes a critical bug that only affects FSA-1000F, FSA-500F and FSA-VM after upgrading to v4.2.1. We strongly recommend that customers who have upgraded to v4.2.1 upgrade to v4.2.2. Customers upgrading from v4.2.0 should upgrade to 4.2.2.

Upgrade Information

Before and after any firmware upgrade

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

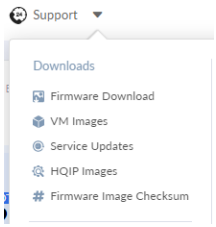
After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox so that web UI screens display properly.

Tracer and Rating Engines

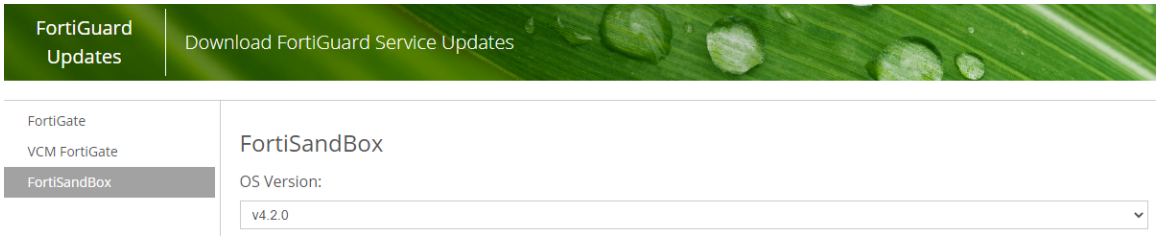
The tracer and rating engines are automatically downloaded by the FortiSandbox from FortiGuard. For air-gapped mode, the engines are available for download from our Support site.

To download the latest engine:

1. Log in to FortiCloud.
2. In the banner, click *Support* > *Service Updates*.



3. On the *FortiGuard Updates* page, click *FortiSandbox* and select the OS version.



Upgrade path

FortiSandbox 4.2.1 officially supports the following upgrade path.

Upgrade from	Upgrade to
4.0.2, 4.2.0	4.2.1
4.0.0-4.0.2	4.2.0
3.2.3	4.0.2
3.2.0–3.2.2	3.2.3
3.1.4	3.2.0
3.0.6–3.1.3	3.1.4
2.5.2–3.0.5	3.0.6
2.4.1–2.5.1	2.5.2
2.4.0	2.4.1

If you are using KVM or Hyper-V, the upgrade path must be 3.1.3 > 3.2.0, then follow the upgrade table.

As with all VM upgrades, take a snapshot or make a checkpoint before upgrading.

After upgrading, FortiSandbox might stop processing files until the latest rating engine is installed either by FDN update or manually. The rating engine is large so schedule time for the download.

Every time FortiSandbox boots up, it checks FDN for the latest rating engine.

If the rating engine is not available or out-of-date, you get these notifications:

- A warning message informs you that you must have an updated rating engine.
- The *Dashboard System Information* widget displays a red blinking *No Rating Engine* message besides *Unit Type*.

If necessary, you can manually download an engine package from Fortinet Customer Service & Support.

If the rating engine is not available or out-of-date, FortiSandbox functions in the following ways:

- FortiSandbox still accepts on-demand, network share, and RPC submissions, but all jobs are pending.
- FortiSandbox does not accept new devices or FortiClients.
- FortiSandbox does not accept new submissions from Sniffer, Device, FortiClient, or Adapter.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Fortinet Customer Service & Support portal located at https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*,

enter the image file name including the extension, and select *Get Checksum Code*.

Upgrading cluster environments

Before upgrading, it is highly recommended that you set up a cluster IP set so the failover between primary (master) and secondary (primary slave) can occur smoothly.

In a cluster environment, use this upgrade order:

1. Upgrade the workers (regular slaves) and install the new rating and tracer engine. Then wait until the devices fully boot up.
2. Upgrade the secondary (primary slave) and install the new rating and tracer engine. Then wait until the device fully boots up.
3. Upgrade the primary (master). This causes HA failover.
4. Install the new rating and tracer engine on the old primary (master) node. This node might take over as primary (master) node.

Upgrade procedure

When upgrading from 3.1.0 or later and the new firmware is ready, you will see a blinking *New firmware available* link on the dashboard. Click the link and you will be redirected to a page where you can either choose to download and install an available firmware or manually upload a new firmware.

Upgrading FortiSandbox firmware consists of the following steps:

1. Download the firmware image from the Fortinet Customer Service & Support portal.
2. When upgrading via the CLI, put the firmware image on a host that supports file copy with the SCP or FTP command. The FortiSandbox must be able to access the SCP or FTP server.
   In a console window, enter the following command string to download and install the firmware image:
   ```
   fw-upgrade -b -s<SCP/FTP server IP address> -u<user name> -t<ftp|scp> -f<file path>
   ```
3. When upgrading via the Web UI, go to *System* > *Dashboard* . In the *System Information* widget, click the *Update* link next to *Firmware Version*. The Firmware Upgrade page is displayed. Browse to the firmware image on the management computer and select the *Submit* button.
4. 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.

FortiSandbox VM firmware

Fortinet provides FortiSandbox VM firmware images for VMware ESXi, Hyper-V, Nutanix, and Kernel Virtual Machine (KVM) virtualization environments.

For more information, see the VM Installation Guide in the Fortinet Document Library.

Product Integration and Support

The following table lists FortiSandbox 4.2.1 product integration and support information.

Web browsers	• Microsoft Edge version 103 • Mozilla Firefox version 101 • Google Chrome version 103 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
FortiManager	• 7.2.0 • 7.0.0 and later • 6.4.0 and later • 6.2.1 and later • 6.0.0 and later
FortiMail	• 7.2.0 • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiClient	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.1 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 7.0.1 • 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
FortiProxy	• 7.0.0 and later • 2.0.0 and later • 1.2.3 and later
FortiWeb	• 7.0.0 and 7.0.1 • 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
AV engine	• 00006.00276
System tool	• 04002.00032
Traffic sniffer	• 00007.00135
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

Resolved Issues

The following issues have been fixed in FortiSandbox 4.2.1. For inquiries about a particular bug, contact Customer Service & Support.

CLI

Bug ID	Description
797957	Fixed missing usage information of `-r` option for `inline-block-timeout` CLI.

GUI

Bug ID	Description
802987	Fixed configuration issue preventing to edit the MACOSX Extensions on *Scan Profile*.
798845	Fixed date range filter on *Log Events*.
823892	Fixed inconsistent job count on *Scan Statistics* widget for *ReadOnly* user profile.
806149	Fixed logon issue when using Radius wildcard and two-factor authentication.

Scan

Bug ID	Description
791867	Improved scan rating logic to override with *Customized Rating* configuration.
783384	Fixed incorrect file typing issue on certain VBS files.
809613	Fixed TCP RST related issues on certain network topology.
821231	Fixed scan logic to stop *Dynamic Scan* when Windows VM unexpectedly shuts down.
802146	Fixed scan logic when *Community Cloud Query* is disabled.
826749	Fixed slow and stuck NetShare scan issue.
818234	Fixed MacOS VM seat count on AWS public cloud deployment.

System & Security

Bug ID	Description
575345	Fixed backup/restore of Memory Yara setting.
801407	Fixed slow engine upgrade download process.
813661	Fixed backup & restore configuration issue on Server Regions of WindowsCloudVM settings.
823031	FortiSandbox generates a lot of *Error happened in FDN update process* error event log.

Logging & Reporting

Bug ID	Description
780041	Fixed datetime format on *Job Report*.
803708	Fixed setting of including *Appendix: System Info* on *Job Report* as enabled by default.
805805	Fixed timestamp format issue with an unnecessary space on *Syslog*.

Common vulnerabilities and exposures

Bug ID	Description
752378	FortiSandbox 4.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2022-30305

Known Issues

The following issues have been identified in FortiSandbox 4.2.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Fabric Integration

Bug ID	Description
810164	ICAP Adapter issue with McAfee Web Gateway responding with 'No Content'

Logging & Reporting

Bug ID	Description
710656	Scheduled detailed report randomly fails to send.
785274	Wrong filename and service info on the Job details of extracted files from FTP traffic via Sniffer mode.

Scan

Bug ID	Description
822024	Unsupported ISO file in UDF 2.5 format not extracted and launched.
828050	Misleading log message warning, *Cannot dispatch file*, on a Cluster deployment used as NetShare scan.

System & Security

Bug ID	Description
818441	Failover sync issue on HA-Secondary unit due to unique certificate.

www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.