

Release Notes

FortiSandbox 4.2.8



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>

FORTINET TRAINING 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 11, 2025

FortiSandbox 4.2.8 Release Notes

34-428-1102553-20250311

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported models	5
New features and enhancements	6
Fabric integration	6
Special Notices	7
Scan Profile	7
Upgrade path	7
Upgrade Information	8
Before and after any firmware upgrade	8
Tracer and Rating Engines	8
Upgrade path	9
Firmware image checksums	9
Upgrading cluster environments	10
Upgrade procedure	10
Downgrading to previous firmware versions	10
FortiSandbox VM firmware	11
Product Integration and Support	12
Resolved Issues	14
Common vulnerabilities and exposures	14

Change Log

Date	Change Description
2025-01-25	Initial release of 4.2.8.
2025-03-05	Updated Resolved Issues on page 14 .
2025-03-11	Updated Resolved Issues on page 14 .

Introduction

This document provides the following information for FortiSandbox version 4.2.8 build 0292.

- [Supported models](#)
- [New features and enhancements](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 4.2.8 Administration Guide* and *FortiSandbox 4.2.8 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

This version contains bug fixes.

Fabric integration

- Added support for FortiManager 7.6.0.

Special Notices

Scan Profile

After upgrading to 4.2.4 the *VM Association* in the *Scan Profile* changes the CSV extension category from *User defined extension* to *Office Documents* as intended. When a CSV file is scanned by the VM, the CSV file type is displayed as *userdefined* in the *Job Detail*.

To work around this issue after upgrade:

1. Go to *Scan Policy and Object > Scan profile*.
2. Click the *VM Association* tab and remove *csv* from the *Office documents category*.
3. Click *Save*.
4. Add *csv* back to the *Office documents category* and click *Save*.
5. Submit a *csv* file to be scanned. The file type will display '*csv*' in the *Job Detail*.

Upgrade path

A feature that was introduced in FortiSandbox v4.2.0 causes a critical bug that only affects FSA-1000F, FSA-500F and VM after upgrading to v4.2.1. We strongly recommend that customers who have upgraded to v4.2.1 upgrade to v4.2.8. Customers upgrading from v4.2.0 should upgrade to 4.2.8.

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*.

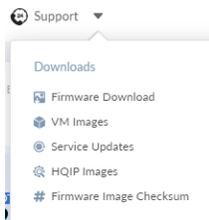
After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox so that web UI screens display properly.

Tracer and Rating Engines

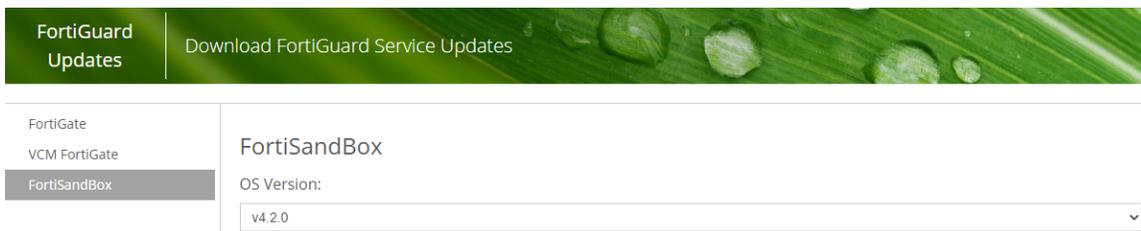
The tracer and rating engines are automatically downloaded by the FortiSandbox from FortiGuard. For air-gapped mode, the engines are available for download from our Support site.

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 4.2.8 officially supports the following upgrade path.

Upgrade from	Upgrade to
4.2.0 – 4.2.7	4.2.8
4.0.0 – 4.0.6	4.2.0



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 4.0.0 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 4.2.8 product integration and support information.

Web browsers	<ul style="list-style-type: none">• Microsoft Edge version 131• Mozilla Firefox version 131• Google Chrome version 131 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.0 and later• 6.4.0 and later
FortiAnalyzer	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.0 and later• 6.4.0 and later
FortiManager	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.0 and later• 6.4.0 and later
FortiMail	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.0 and later
FortiClient	<ul style="list-style-type: none">• 7.2.0• 7.0.0 and later
FortiEMS	<ul style="list-style-type: none">• 7.2.0• 7.0.0 and later
FortiADC	<ul style="list-style-type: none">• 7.2.0• 7.1.0 and 7.1.1• 7.0.0 and 7.0.3• 6.2.0 and later• 6.1.0 and later• 6.0.0 and later
FortiProxy	<ul style="list-style-type: none">• 7.2.1 and later• 7.0.0 and later• 2.0.0 and later
FortiWeb	<ul style="list-style-type: none">• 7.2.0• 7.0.0 and later
Fortisolator	<ul style="list-style-type: none">• 2.4.2
AV engine	<ul style="list-style-type: none">• 00006.00298
System tool	<ul style="list-style-type: none">• 04002.00045

Traffic sniffer

- 00007.00138

Virtualization environment

- VMware ESXi:
 - Intel CPU server: 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.1
 - AMD CPU server: 6.7 and 7.0.1
- KVM: Linux version 4.15.0 qemu-img v2.5.0
- Microsoft Hyper-VWindows server 2016, 2019, and 2022

Resolved Issues

The following issues have been fixed in FortiSandbox 4.2.8. For inquiries about a particular bug, contact [Customer Service & Support](#).

Common vulnerabilities and exposures

	Description
1051926	FortiSandbox 4.2.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2024-6387
1071711	FortiSandbox4.2.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2024-52960
1071714	FortiSandbox 4.2.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2024-54027
1072285	FortiSandbox4.2.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2024-52961



www.fortinet.com

Copyright© 2025 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.