

# Release Notes

## FortiSandbox 4.4.8



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<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 LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



February 10, 2026

FortiSandbox 4.4.8 Release Notes

34-448-1196937-20260210

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>New features and enhancements</b> .....	<b>6</b>
System & Security .....	6
<b>Special Notices</b> .....	<b>7</b>
Web Category Updates .....	7
<b>Upgrade Information</b> .....	<b>8</b>
Before upgrade .....	8
After upgrade .....	8
Tracer and Rating Engines .....	8
Rating engine .....	9
Upgrade path .....	9
500G and 1500G models .....	10
Firmware image checksums .....	10
Upgrading cluster environments .....	10
Upgrade procedure .....	10
Downgrading to previous firmware versions .....	11
FortiSandbox VM firmware .....	11
Scan Profile .....	11
Supported models .....	12
<b>Product Integration and Support</b> .....	<b>13</b>
<b>Resolved Issues</b> .....	<b>15</b>
GUI .....	15
Scan .....	15
System & Security .....	15
CLI .....	15
Common vulnerabilities and exposures .....	16

# Change Log

Date	Change Description
2025-10-09	Initial release.
2025-12-09	Updated <a href="#">Resolved Issues on page 15</a> .
2026-02-10	Updated <a href="#">Resolved Issues on page 15</a> .

# Introduction

This document provides the following information for FortiSandbox version 4.4.8 build 0412.

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

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 4.4.8 Administration Guide* and *FortiSandbox 4.4.8 VM Install Guide*.

# New features and enhancements

The following is summary of new features and enhancements in version 4.4.8. For details, see the [FortiSandbox 4.4.8 Administration Guide](#) in the [Fortinet Document Library](#).

## System & Security

- Improved job configuration protection to prevent evasion of malware detection.

# Special Notices

## Web Category Updates

Since v4.4.0, several Web Categories are updated from *Clean* to *Low Risk*. Refer to [Web Category](#) for the updated list. When a job contains or links to a URL rated as *Low Risk*, then the job will be forwarded to the Dynamic VM Scan in order to check and possibly elevate the rating. However, this increases the jobs entering the VM. If the deployed system does not have the capacity to handle the increase, either override some categories to *Clean* as appropriate or increase selective categories to *Medium Risk*.

# Upgrade Information

## Before upgrade

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

### If you intend to use the new VMs after upgrade:

Ensure you have the appropriate VM licenses. Activating a VM requires the license specific to the version you are using with the equal number of clones. For example, if you have Win11 and Office 2021 activation keys you can use those keys to run the *Win11O21 VM*. If you want to configure 10 clones, then you will need 10 licenses.

Keep the following considerations in mind:

- We recommend purchasing a new license, downloading the VMs, and then reassigning the clones.
- If you download the new VMs (without updating your license) and then remove existing clones to make room for new ones, the old license will not work.

For more information about license keys, see *VM Settings > Optional VMs* in the *FortiSandbox Administration Guide*.

## After upgrade

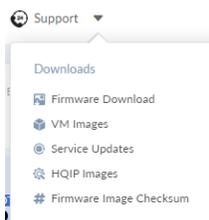
After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox so that web UI screens display properly.

## Tracer and Rating Engines

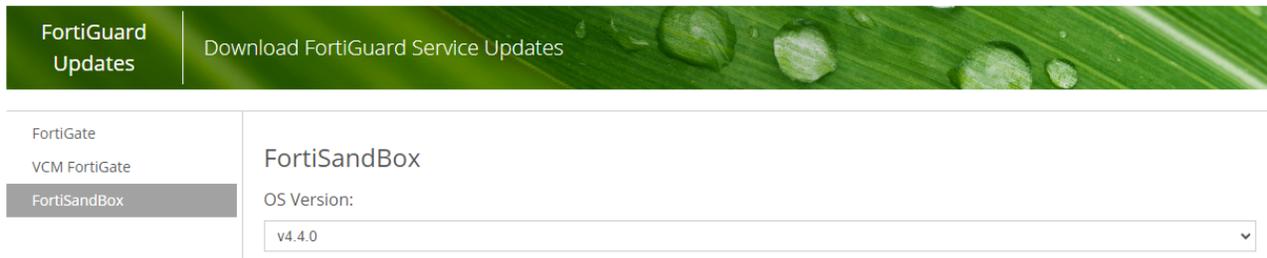
The tracer and rating engines are automatically downloaded by the FortiSandbox from FortiGuard. For air-gapped mode, the engines are available for download from our Support site.

### 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.



## Rating engine

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.



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.

## Upgrade path

FortiSandbox 4.4.8 officially supports the following upgrade path.

Upgrade from	Upgrade to
4.4.0 - 4.4.7	4.4.8
4.2.0 - 4.2.7	4.4.0
4.0.0 - 4.0.5	4.2.0



When upgrading from 4.4.0, 4.4.1 and 4.4.2, the configuration of *ws-auth* will be reset to *enabled*.

---



If you are upgrading from 4.2.0 – 4.2.3 to 4.2.4, see [Scan Profile](#) below.

---

## 500G and 1500G models

For 500G and 1500G models the upgrade path is: *v4.2.5 NPI* build to *v4.4.3 build 0380* to *v4.4.8 build 0412*.

## 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](#).

## 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*.

## Supported models

FortiSandbox	FSA-500F, FSA-500G, FSA-1000F/-DC, FSA-1500G, FSA-2000E, FSA-3000E, and FSA-3000F
FortiSandbox-VM	Hyper-V, KVM, Nutanix and VMware ESXi.

# Product Integration and Support

The following table lists FortiSandbox 4.4.8 product integration and support information. FortiSandbox integration and support is tested based on the firmware image of the product's latest available GA build during the release testing process. FortiSandbox also supports backwards compatibility to the product's earlier GA builds.



This minor patch addresses a limited set of vulnerabilities and issues. In line with our standard patch process, it does not include full integration testing. Instead, we rely on the validation results from the previous release, where comprehensive testing was performed with the available builds at that time. Generally, newer patch releases of supported products maintain backward compatibility, and their integration can reasonably be assumed to function as expected. Repeating full integration testing across all products and versions for every minor update would introduce significant complexity and is not part of our regular patch workflow.



FortiSandbox integration and support is tested on the firmware image of the product's major release (7.0.0, 7.2.0, 7.4.0 etc). Minor releases (7.0.1, 7.0.2, 7.0.3 etc) are not individually tested because they are based on the same firmware image.

Where indicated, version *x.x.x and later* means integration and support is based on the major version, including minor versions unless otherwise indicated in the *Administration Guide* or *Release Notes*.

<b>Web browsers</b>	<ul style="list-style-type: none"><li>• Google Chrome version 140</li><li>• Microsoft Edge version 140</li><li>• Mozilla Firefox version 143</li></ul> Other web browsers may function correctly but are not supported by Fortinet.
<b>FortiOS/FortiOS Carrier</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiMail</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>

<b>FortiClient</b>	<ul style="list-style-type: none"> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> <li>• 6.4.0 and later</li> </ul>
<b>FortiEMS</b>	<ul style="list-style-type: none"> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> <li>• 6.4.0 and later</li> </ul>
<b>FortiADC</b>	<ul style="list-style-type: none"> <li>• 7.4.0 and later</li> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> <li>• 6.2.0 and later</li> <li>• 6.1.0 and later</li> <li>• 6.0.0 and later</li> <li>• 5.4.0 and later</li> </ul>
<b>FortiProxy</b>	<ul style="list-style-type: none"> <li>• 7.4.0 and later</li> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> <li>• 2.0.0 and later</li> </ul>
<b>FortiWeb</b>	<ul style="list-style-type: none"> <li>• 7.4.0 and 7.4.1</li> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> </ul>
<b>Fortisolator</b>	<ul style="list-style-type: none"> <li>• 2.4.3 and later</li> </ul>
<b>FortiEDR</b>	<ul style="list-style-type: none"> <li>• 5.2.0 and later</li> </ul>
<b>AV engine</b>	<ul style="list-style-type: none"> <li>• 00007.00025</li> </ul>
<b>FortiSandbox System tool</b>	<ul style="list-style-type: none"> <li>• 04004.00079</li> </ul>
<b>Traffic Sniffer Engine</b>	<ul style="list-style-type: none"> <li>• 00007.00183</li> </ul>
<b>Virtualization environment</b>	<ul style="list-style-type: none"> <li>• VMware ESXi: 5.1, 5.5, 6.0, 6.5, 6.7, 7.0.1, and 8.0</li> <li>• KVM: Linux version 4.15.0 qemu-img v2.5.0</li> <li>• Microsoft Hyper-V: Windows server 2016, 2019, and 2022</li> </ul>

# Resolved Issues

The following issues have been fixed in FortiSandbox 4.4.8. For inquiries about a particular bug, contact [Customer Service & Support](#).

## GUI

Bug ID	Description
1180603	Fixed an internal server error that occurred when accessing the System > FortiGuard tab.

## Scan

Bug ID	Description
1196525	Fixed RTAP query when in Air-gapped mode.

## System & Security

Bug ID	Description
1117701	Fixed failed remote server backups on Secondary and Worker nodes.
1166689	Fixed missing entries (fsaTrapLKDN and fsaTrapLKUP) in the MIB file descriptions.
1202816	Fixed the read-only privileges to prevent users from modifying system configurations by simulating valid requests.

## CLI

Bug ID	Description
1195364	Fixed an issue where FortiSandbox failed to create a read-only LDAP admin via CLI without requiring a password.

## Common vulnerabilities and exposures

Bug ID	Description
1172018	FortiSandbox 4.4.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-53679</li></ul>
1172622	FortiSandbox 4.4.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-53949</li></ul>
1129746	FortiSandbox 4.4.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-26466</li></ul>
1172621	FortiSandbox 4.4.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-54353</li></ul>
1119938	FortiSandbox 4.4.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-52436</li></ul>



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2026 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 Chief Legal Officer, 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.