FORTINET

Release Notes

FortiSandbox 4.4.5

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

April 09, 2024
FortiSandbox 4.4.5 Release Notes
34-445-1012474-20240409

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
New features and enhancements **6**
Scan 6
Special Notices **7**
Web Category Updates 7
Upgrade Information **8**
Before upgrade 8
After upgrade 8
Tracer and Rating Engines 8
Upgrade path 9
Firmware image checksums 10
Upgrading cluster environments 10
Upgrade procedure 11
Downgrading to previous firmware versions 11
FortiSandbox VM firmware 11
Scan Profile 11
Supported models 12
Product Integration and Support **13**
Resolved Issues **15**
GUI 15
Device 15
Logging & Reporting 15
Common vulnerabilities and exposures 15

Change Log

Date	Change Description
2024-03-29	Initial release.
2024-04-09	Updated Resolved Issues on page 15.

Introduction

This document provides the following information for FortiSandbox version 4.4.5 build 0393.

- 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 4.4.5 Administration Guide* and *FortiSandbox 4.4.5 VM Install Guide*.

New features and enhancements

The following is summary of new features and enhancements in version 4.4.5. For details, see the *FortiSandbox4.4.5 Administration Guide* in the Fortinet Document Library.

Scan

- Added support for Inline Block Policy in FortiProxy.

Special Notices

Web Category Updates

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

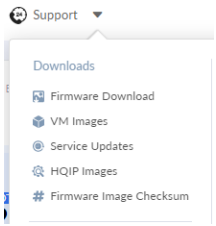
After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox so that web UI screens display properly.

Tracer and Rating Engines

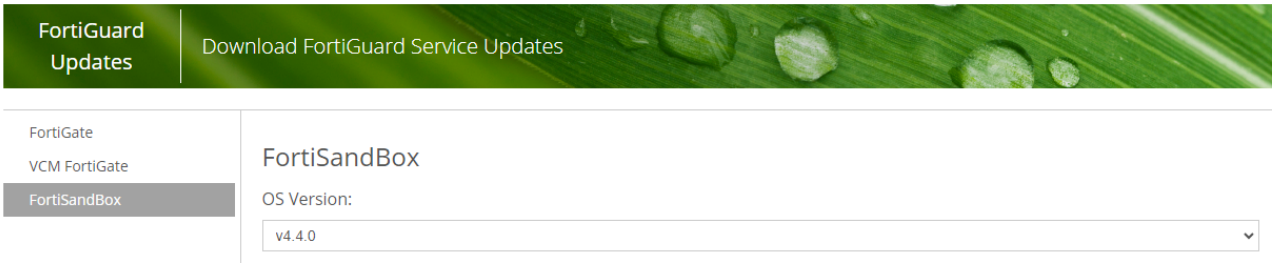
The tracer and rating engines are automatically downloaded by the FortiSandbox from FortiGuard. For air-gapped mode, the engines are available for download from our Support site.

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.



Upgrade path

FortiSandbox 4.4.5 officially supports the following upgrade path.

Upgrade from	Upgrade to
4.4. 0 - 4.4.4	4.4.5
4.2.0 - 4.2.7	4.4.0
4.0.0 - 4.0.5	4.2.0
3.2.4	4.0.4
3.2.0 - 3.2.3	3.2.4

FortiSandbox PaaS is not supported by the main trunk. Please visit the FortiSandbox PaaS page for the latest upgrade information.

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.

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.

Automatic Upgrade:

The GUI recommended upgrade path does not support upgrading FortiSandbox for GCP and OCI from v4.2.3 to v4.2.4 and higher.

Workaround:

GCP and OCI platforms only support upgrade from v 4.2.3 GA directly to 4.4.0 GA.

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.

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-2000E, FSA-3000E, FSA-500F, FSA-1000F/-DC, FSA-3000F, FSA-500G, and FSA-1500G
FortiSandbox-VM	AWS, Azure, Hyper-V, KVM, VMware ESXi, GCP and OCI

Product Integration and Support

The following table lists FortiSandbox 4.4.5 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.

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*.

Web browsers	• Google Chrome version 121 • Microsoft Edge version 121 • Mozilla Firefox version 122 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiAnalyzer	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiMail	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiClient	• 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiEMS	• 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiADC	• 7.4.0 and later

	• 7.2.0 and later • 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
FortiProxy	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 2.0.0 and later
FortiWeb	• 7.4.0 and 7.4.1 • 7.2.0 and later • 7.0.0 and later
FortiIsolator	• 2.4.3 and later
FortiEDR	• 5.2.0 and later
AV engine	• 00006.00295
FortiSandbox System tool	• 4004.00073
Traffic Sniffer Engine	• 00007.00169
Virtualization environment	• VMware ESXi: 5.1, 5.5, 6.0, 6.5, 6.7, 7.0.1, and 8.0 • KVM: Linux version: 4.15.0 qemu-img v2.5.0 • Microsoft Hyper-V: Windows server 2016, 2019, and 2022

Resolved Issues

The following issues have been fixed in FortiSandbox 4.4.5. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
1012696	Fixed the device name error in the *Inline Block Policy* for FortiProxy.

Device

Bug ID	Description
1012736	Fixed the VM screenshot feature in FSA-VM GCP.
1011181	Fixed changing the DNS server setting in FSA-VM Azure so it does not revert after rebooting the device.

Logging & Reporting

Bug ID	Description
1006501	Resolved a reports issue where Radius admins could not generate reports.

Common vulnerabilities and exposures

Bug ID	Description
1007264	FortiSandbox 4.4.5 is no longer vulnerable to the following CVE Reference: • CVE-2024-31487

www.fortinet.com