FORTINET

Release Notes

FortiSandbox 4.2.3

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 4.2.3 Release Notes
34-423-833080-20230412

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-11-16	Initial release.
2022-11-28	Updated Known Issues on page 16.
2022-11-29	Updated Special Notices on page 7.
2023-03-22	Updated Known Issues on page 16.
2023-04-12	Updated Resolved Issues on page 14.

Introduction

This document provides the following information for FortiSandbox version 4.2.3 build 0255.

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 4.2.3 Administration Guide* and *FortiSandbox 4.2.3 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 4.2.3. For details, see the *FortiSandbox4.2.3 Administration Guide* in the Fortinet Document Library.

CLI

- Enhanced `tac-report` CLI to provide more output of `diagnose-sys-perf` different time ranges. See, Diagnose commands.
- Enhanced `vm-license` CLI to include additional license information. See, vm-license.

GUI

- Support *User Defined File* type as a group of configured file extensions on the File Statistics widget.

Fabric integration

- Added a RESTAPI to query pending job count.
- Added replacement message on Sniffer Mode when *TCP Reset* is enabled. See, Sniffer.

Scan

- Added csv file support on Microsoft Office scan profile group.
- Enhanced Network Share scan logic on handling 10K files (conserve mode).
- Increased VM memory size on VM00, 500F and 1000F models to improve scan performance.
- Introduced a new Optional VM 'WIN10O19V1' based on Windows 10 with Office 2019.

System & Security

- Show disclaimer message on SSH session. See, Login Disclaimer.

Special Notices

DNS server setting

The DNS server setting for port3 is unused and it falls back to system DNS. When this occurs, DNS resolution initiated by the VMs will go through system DNS. The issue exists only on v4.2.3 GA release that has the upgraded DNS daemon. A fix is available on a special build and can be requested via Support team.

Scan Profile

After upgrading to 4.2.3 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 v4.2.2. 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*.

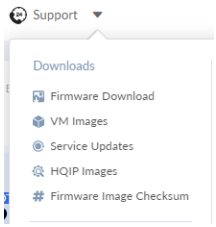
After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox so that web UI screens display properly.

Tracer and Rating Engines

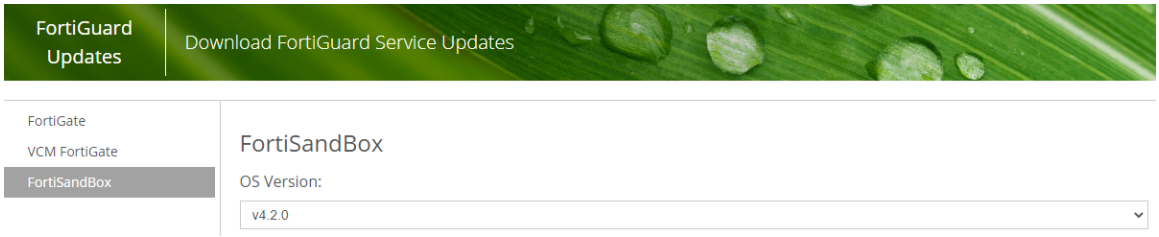
The tracer and rating engines are automatically downloaded by the FortiSandbox from FortiGuard. For air-gapped mode, the engines are available for download from our Support site.

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 4.2.3 officially supports the following upgrade path.

Upgrade from	Upgrade to
4.2.0–4.2.2	4.2.3
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 4.2.3 product integration and support information.

Web browsers	• Microsoft Edge version 106 • Mozilla Firefox version 106 • Google Chrome version 106 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 7.2.0 and later • 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 and later • 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 and later • 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	• 7.2.0 and later • 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 laster • 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	• 7.1.0 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 • 5.4.0 and later • 5.3.0 and later • 5.0.1 and later
FortiProxy	• 7.2.1 • 7.0.0 and later • 2.0.0 and later • 1.2.3 and later
FortiWeb	• 7.0.0 and later • 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	• 00006.00282
System tool	• 04002.00041
Traffic sniffer	• 00007.00138
Virtualization environment	• VMware ESXi (Intel CPU): 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 4.2.3. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
831413	Fixed admin profile read-write issue on the dashboard widget to perform firmware upgrade.
848249	Fixed *Data Error Found on page 1*' display error due to wrong input type.
849447	Fixed missing firmware upgrade button when logon as LDAP or Radius wildcard administrator.

Scan

Bug ID	Description
779904	Fixed return value on FortiMail submission of encrypted archive files with no matching password.
829063, 829063, 829272, 845934	Fixed stuck scan issue due to a race condition when in Pipeline mode showing *Holding future VM scan to let VMs cool down* message.
855887	Fixed unexpected VM scan termination issue when in Pipeline mode causing performance issue and repeated *Failed to get tracer_log.tar* on the event log.

System & Security

Bug ID	Description
828138	Extended maximum *Primary Secret Key* digits support of up to 32 when authenticating Radius wildcard.
837489	Fixed inability to logon after upgrade of HA devices from 4.2.0 to either 4.2.1 or 4.2.2.
854159	Fixed alternate SMTP port 465 for cloud community file submission.

Logging & Reporting

Bug ID	Description
710656	Fixed random failure to send the scheduled detailed report.
824716	Fixed file name field on FortiNDR logs.
828456	Fixed missing log even when power supply goes offline and online.
831018, 835408	Fixed host name value of the CEF syslog.

Common vulnerabilities and exposures

Bug ID	Description
795171	FortiSandbox 4.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2022-27487

Known Issues

The following issues have been identified in FortiSandbox 4.2.3. 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
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.

System & Security

Bug ID	Description
818441	Failover sync issue on HA-Secondary unit due to unique certificate.
857120	DNS server setting for port3 is unused and it falls back to system DNS. For more information, see Special Notices on page 7.

www.fortinet.com