FortiSandbox - Release Notes

Version 3.2.3

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

November 19, 2021
FortiSandbox 3.2.3 Release Notes
34-323-713665-20211119

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-08	Initial release.
2021-08-04	Updated Resolved Issues on page 12.
2021-10-06	Updated Resolved Issues on page 12.
2021-10-14	Updated Upgrade Information on page 7.
2021-11-19	Updated Known Issues on page 14.

Introduction

This document provides the following information for FortiSandbox version 3.2.3 build 0255.

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.2.3 Administration Guide* and *FortiSandbox 3.2.3 VM Install Guide*.

Supported models

FortiSandbox version 3.2.3 supports the FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3500D, FSA-3000E, and FSA-VM (AWS, Azure, Hyper-V, KVM, and VMware ESXi) models.

New features and enhancements

The following is a list of new features and enhancements in version 3.2.3:

- Support Custom-VM license as perpetual-based license. Previously, this was subscription-based license.
- New CLI command to cancel processing jobs.
- Support for configuring Cluster IP on aggregate interface for the bandwidth and redundancy of file submission.

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.

Upgrade path

FortiSandbox 3.2.3 officially supports the following upgrade paths.

Upgrade from	Upgrade to
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

You will need to create a disk if you are using FortiSandbox on Azure with Pay As You Go and upgrading from a version prior to v3.2.0. See Creating a data disk.

If you are using KVM or Hyper-V, the upgrade path must be 3.1.3 > 3.2.0 > 3.2.3.
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 engine. Then wait until the devices fully boot up.
2. Upgrade the secondary (primary slave) and install the new rating engine. Then wait until the device fully boots up.
3. Upgrade the primary (master). This causes HA failover.
4. Install the new rating 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 3.2.3 product integration and support information.

Web browsers	• Microsoft Edge version 90 • Mozilla Firefox version 89 • Google Chrome version 91 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 7.0.0 • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later
FortiAnalyzer	• 7.0.0 • 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	• 7.0.0 • 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
FortiADC	• 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
FortiClient	• 7.0.0 • 6.4.0 and later • 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiEMS	• 7.0.0 • 6.4.0 and later • 6.2.0 and later • 6.0.5 and later
FortiMail	• 7.0.0

	• 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.4.0 and later
FortiProxy	• 2.0.0 and later • 1.2.3 and later
FortiWeb	• 6.4.0 • 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	• 00006.00263
Tracer engine	• 03002.00022
System tool	• 03002.00052
Traffic sniffer	• 00004.00036
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 3.2.3. For inquiries about a particular bug, contact Customer Service & Support.

Fabric Integration

Bug ID	Description
688659	Improved intermittent connection issue with the community cloud.
689623	Fixed connectivity issues with FortiClient that randomly gets stalled.

GUI

Bug ID	Description
687401	Fixed wrong CPU data on the *System Resource Usage* widget.
690948	Fixed logon to the Web GUI with RADIUS two-factor authentication.
690033	Fixed GUI logon using multi-factor authentication with FortiToken.
716577	Fixed login failure with remote wildcard user which includes character '@'.

Scan

Bug ID	Description
687843	Fixed a race condition when processing results from cluster nodes.
686146	Fixed wrong behavior of handling YARA rules with *clean* risk level of 0 and 1.

System & Security

Bug ID	Description
692151	Fixed high disk usage on FSA-VM environment.

Log & Report

Bug ID	Description
694771	Fixed display issue of long and sub URL.
690564	Fixed syslog format to include `host_id` after timestamp to conform to RFC.

Common vulnerabilities and exposures

Bug ID	Description
680722	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-24010
680723	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-26097
675153	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-26096
683305	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-26098
680720 680785 680787 681362 681363 681364 681630 681633	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-24014
680721	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2020-29011
697271	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-24010
684391	FortiSandbox 3.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-26105

Known Issues

The following issues have been identified in FortiSandbox 3.2.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Scan

Bug ID	Description
653559	The guest mouse pointer is misaligned in Interactive mode. Fixed in 4.0.0.
672997	Sniffer mode fails to extract user-defined file type `eml` from the traffic.
677043	Sniffer mode incorrectly extracts the URL in some cases.
682154	Missing job details info due to retention policy discrepancies caused by heavy load. Fixed in 4.0.0.

System & Security

Bug ID	Description
681038	Small footprint of memory leak on prescan daemon. Fixed in 4.0.0.
761582	Licensing issue after applying the perpetual-based Custom-VM license. (Request a special build from Support team for the fix).