FortiSandbox - Release Notes

Version 3.2.1

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 20, 2020
FortiSandbox 3.2.1 Release Notes
34-321-631295-20200820

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-08-20	Initial release.

Introduction

This document provides the following information for FortiSandbox version 3.2.1 build 0222.

- Supported models
- New features and enhancements
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.2.1 Administration Guide* and *FortiSandbox 3.2.1 VM Install Guide*.

Supported models

FortiSandbox version 3.2.1 supports the FSA-500F, FSA-1000D, FSA-1000F, FSA-1000F-DC, 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 3.2.1:

- Redefined HA-Cluster node types and Scan Filter List type.
  - `master` is renamed to `primary`
  - `primary slave` is renamed to `secondary`
  - `regular slave` is renamed to `worker`
  - `white list` is renamed to `allowlist`
  - `black list` is renamed to `blocklist`
- Enhanced Bit9 Adapter Configuration and Connectivity.
- Support backing up CustomVM images to remote server via CLI.
- Windows XP, including custom Windows XP, is no longer supported. FortiSandbox no longer supports scanning samples in Windows XP.
  - If there are Windows XP enabled, you cannot upgrade to version 3.2.1. You must first set its clone number to *0* and migrate it to use Windows 7 or later.
  - In *Scan Policy > Scan Profile* in the *VM Association* tab, if you try to change any WinXP file extension, a message informs you that WinXP is no longer supported.
  - In *Virtual Machine > VM Images*, if you try to change a WinXP clone number to a higher number or try to activate a WinXP image, a message informs you that WinXP is no longer supported.
  - In Rescue Mode, if WinXP is enabled and you try to do a system upgrade, a message informs you that WinXP is no longer supported.
  - In CLI, if WinXP is enabled and you try to update an image or install a custom Win XP image, a message informs you that WinXP is no longer supported.
  - If you try upgrade using CLI, Rescue Mode, or manually from any version other than 3.2.0, a message informs you that you must upgrade to 3.2.0 first.

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

⚠ If you are using KVM or Hyper-V, the upgrade path must be 3.1.3 > 3.2.0 > 3.2.1.
As with all VM upgrades, take a snapshot or make a checkpoint before upgrading.

FortiSandbox 3.2.1 officially supports upgrading directly from version 3.2.0.

To upgrade from other versions, see the following table.

Upgrading from	Upgrade path
3.0.6–3.1.3	3.0.6–3.1.3 > 3.2.0 > 3.2.1
3.0.0–3.0.5	3.0.0–3.0.5 > 3.0.6 > 3.1.2 > 3.2.0 > 3.2.1
2.5.0–2.5.1	2.5.0–2.5.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0 > 3.2.1
2.4.0	2.4.0 > 2.4.1 > 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0 > 3.2.1
2.3.0–2.3.2	2.3.0–2.3.2 > 2.3.3 > 2.4.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0 > 3.2.1
2.2.1 or earlier	2.2.1 > 2.2.2 > 2.3.0 > 2.3.3 > 2.4.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0 > 3.2.1

⚠ 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 3.2.1 product integration and support information.

Web browsers	• Microsoft Edge version 84 • Mozilla Firefox version 78 • Google Chrome version 84 Other web browsers may function correctly but are not supported by Fortinet.
FortiAnalyzer	• 6.4.2 • 6.4.0 and later (all FortiSandbox models except FSA-1000F-DC) • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.8 and later
FortiADC	• 6.0.0 • 5.4.0 and later • 5.3.0 and later • 5.0.1 and later
FortiClient	• 6.4.0 • 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiEMS	• 6.4.0 • 6.2.0 and later • 6.0.5 and later
FortiMail	• 6.4.2 • 6.4.0 • 6.2.0 and later • 6.0.0 and later • 5.4.0 and later • 5.3.0 and later • 5.2.0 and later
FortiManager	• 6.4.2 • 6.2.1 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later
FortiOS/FortiOS Carrier	• 6.4.2

	• 6.2.0 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later
FortiWeb	• 6.3.5 • 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
FortiProxy	• 1.2.3
AV engine	• 6.00247
Tracer engine	• 3002.00022
System tool	• 3002.00043
Virtualization environment	• VMware ESXi: 5.1, 5.5, 6.0, or 6.5 and later • KVM: Linux version 4.15.0 qemu-img v2.5.0 • Microsoft Hyper-V: Windows server 2016

Resolved Issues

The following issues have been fixed in FortiSandbox 3.2.1. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
641720	Fixed GUI logon delay when a Global Network's contributor is unreachable.

Logging & Reporting

Bug ID	Description
644619	Fixed source IP address in the message log of ICAP file submission.

Scan

Bug ID	Description
628544	Support password-protected on NetShares' archives.
637816	Fixed random timeout result issue for FortiMail URL submission.
638353	Fixed job scan flow during FortiGuard update causing wrong rating.
643370	Fixed allowlist and blocklist limits.
645500	Fixed encoding support of MTA's email body.

System & Security

Bug ID	Description
596636	Removed standard ports from the Adapter port settings.
606249	Fixed VM activation failure in Hyper-V.
620331, 622675	Fixed partial config lost after firmware upgrade.
643265	Fixed manual upgrade handling of AV package.
645837	Fixed system stability when many FortiClient endpoints download malware package.
649569	Fixed network share overloading issue. With a large number of files, network share scan cannot completely finish and doesn't list all jobs.
655409	Fixed random failure on downloading FortiGuard engine and package.

Known Issues

The following issues have been identified in FortiSandbox 3.2.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

System & Security

Bug ID	Description
575345	Memory YARA setting is not supported on backup and restore.
627458	High CPU utilization issue on 3500D and 1000D with full Win10 VMs.
658816	Upgrading Hyper-V might occasionally fail.