FORTINET

Release Notes

FortiSandbox 4.2.0

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 4.2.0 Release Notes
34-420-753665-20230412

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-04-12	Initial release.
2022-04-26	Updated Resolved Issues on page 15.
2022-06-14	Updated Resolved Issues on page 15.
2022-11-16	Updated Resolved Issues on page 15.

Introduction

This document provides the following information for FortiSandbox version 4.2.0 build 0192.

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 4.2.0 Administration Guide* and *FortiSandbox 4.2.0 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 4.2.0. For details, see the *FortiSandbox4.2.0 Administration Guide* in the Fortinet Document Library.

GUI

- Introduced *Scan Performance* page for tracking historical usages.
- Introduced Custom VM modification within FortiSandbox.
- Upgraded GUI framework to Neutrino.
- Added FortiAnalyzer on the *Connectivity* widget.
- Added FortiNDR on the *Connectivity* widget.
- Added *Last 7 days* option to *System Resources Usage* widget.
- Added recorded video link on *Job Detail* page.

Fabric integration

- Introduced Inline Blocking feature with FortiGate FortiOS 7.2.
- Introduced multiple ICAP adapter profile for multi-tenancy support.
- Added *hold*" option to ICAP adapter deployment.
- Added configuration of aggregate interface via JSON RPC.
- Added option to download Macro content via JSON RPC.
- Re-introduced FortiAI as FortiNDR with new network response detection features.
- Supported FP/FN marking via JSON RPC including auto submission to Fortinet.
- Supported sending TCP RST on *Sniffer* mode deployment.
- Supported system resource check via API.

Scan

- Introduced *Configurable Internet Browser* on *Dynamic Scan*.
- Introduced *Pipeline Scan Mode* for reducing VM maintenance overhead.
- Introduced *Rating Engine Service* mode to improve performance.
- Added hot-standby VMs on AWS and Azure cloud deployment for improving performance.
- Combined the tracer engines for Windows, Android and Linux into a single engine.
- Enhanced log tracking on *Dynamic Analysis* for resiliency.
- Improved performance of email relay with MTA adapter.

- Improved handling of similar URL when its payload has changed.
- Adjusted *Dynamic Scan* timeout value with a minimum of 30 seconds on high-end models.

System & Security

- Checked system time discrepancy on HA-Cluster deployment and logged a Warning event.
- Supported backup, restore and revision of the configuration.
- Upgraded OpenSSL library.
- Expanded custom Linux VM support on public cloud.

Logging & Reporting

- Introduced customizable reports for white-labelling.
- Added *Submit Time*, *Rated By* and *File Type* fields on the FortiAnalyzer logs.
- Enhanced naming results shown on *Rated By* of the job reports.
- Send periodic log of *Scan Statistics* to FortiAnalyzer.
- Send periodic log of *System Resource* usages to FortiAnalyzer.

CLI

- Enhanced `device-authorization` to enable/disable inline-block on FortiGate.
- Enhanced `test-network` to check FortiAnalyzer, Cloud VM, and Public Cloud internal connectivity.
- Enhanced `show` command to list the HC external IP.
- Updated `tac-report` relating to new features on this release.
- Added `device-clean-pdf` to enable/disable FortiSandbox to generate PDF report for clean rating jobs when requested by device.

Special Notices

Tracer engine error

When a Proxy is configured under *FortiGuard* > *FortiSandbox Community Cloud & Threat Intelligence Settings* the URL Scan returns the following error: *Tracer Error: Error happens in rating engine*.

To work around this issue:

1. Go to *System* > *FortiGuard.*
2. Under *FortiSandbox Community Cloud & Threat Intelligence Settings*, disable *Use Proxy*.
3. Reboot FortiSandbox to reset the rating engine configuration.

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*.

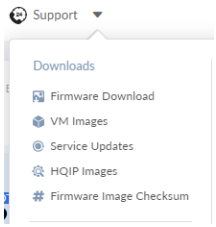
After any firmware upgrade, if you are using the web UI, clear the browser cache before logging into FortiSandbox so that web UI screens display properly.

Tracer and Rating Engines

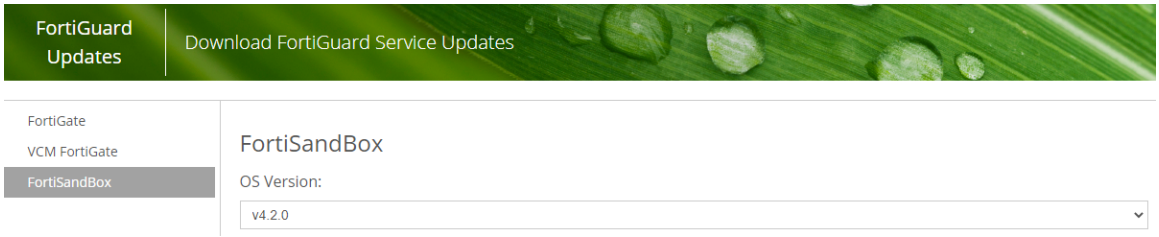
The tracer and rating engines are automatically downloaded by the FortiSandbox from FortiGuard. For air-gapped mode, the engines are available for download from our Support site.

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 4.2.0 officially supports the following upgrade path.

Upgrade from	Upgrade to
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 4.2.0 product integration and support information.

Web browsers	• Microsoft Edge version 99 • Mozilla Firefox version 98 • Google Chrome version 98 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 7.2.0 • 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 • 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 • 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	• 7.0.0 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 later • 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	• 7.0.0 and later • 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	• 7.0.0 and later • 2.0.0 and later • 1.2.3 and later
FortiWeb	• 7.0.0 • 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	• 00006.00266
System tool	• 04002.00019
Traffic sniffer	• 00005.00239
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 4.2.0. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
755708	Fixed admin profile read-write issue on the dashboard widget to perform firmware upgrade.

Fabric integration

Bug ID	Description
774786	Fixed encoding issue of unicode characters on API query of job detail.
770796	Fixed content-type changed issue on NetShare scan of AWS deployment.
764185	Fixed broken web page issue on ICAP deployment due to no encoding support.
790423	FortiSandbox fails to download packages from FortiManager. For details, see Special Notices.

HA Cluster

Bug ID	Description
694610	Issues about cluster external/internal interface

Scan

Bug ID	Description
780955	Fixed download tracer log for failed scan.
760045	Fixed override server issue on web filtering query.
774122	Fixed timeout issue on custom RHEL8 VM due to lack of memory resource.

System & Security

Bug ID	Description
783344	Fixed conserve mode state issue due to undefined limit on sniffer mode deployment specific to 3000F model.
694610	Fixed configuration issue that allows using similar interface for both external and internal networking.
783889	Fixed gratuitous ARP issue on HA-cluster fail-back scenario.
792003	Fixed configuration synchronization issue of SNMP to secondary unit.
668581	Upgraded JQuery library to latest stable version.
742300	Fixed booting hung issue after executing factory-reset.
783889	Fixed gratuitous ARP issue on HA-cluster fail-back scenario.

Logging & Reporting

Bug ID	Description
764486	Fixed wrong timezone issue on syslog (e.g. FortiSIEM).
707073	Fixed missing system event log for downloading job details such as Tracer Package.

Common vulnerabilities and exposures

Bug ID	Description
683306	FortiSandbox4.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2022-26115
719039	FortiSandbox4.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2022-22305

Known Issues

The following issues have been identified in FortiSandbox 4.2.0. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Logging & Reporting

Bug ID	Description
710656	Scheduled detailed report randomly fails to send.

System & Security

Bug ID	Description
575345	*Known Memory Yara* setting is not supported on *backup*/*restore*.

www.fortinet.com