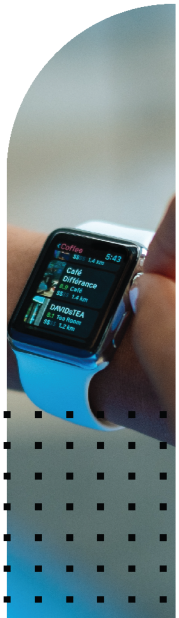
Release Notes

FortiSandbox 4.0.0



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

FORTINET®

September 08, 2021
FortiSandbox 4.0.0 Release Notes
34-400-662447-20210908

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-04-19	Initial release.
2021-07-08	Added Common vulnerabilities and exposures on page 16.
2021-07-08	Updated supported FortiManager versions in Product Integration and Support on page 12.
2021-08-04	Updated Resolved Issues on page 14.
2021-08-25	Updated Product Integration and Support on page 12.

Introduction

This document provides the following information for FortiSandbox version 4.0.0 build 0040.

- 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 4.0.0 Administration Guide* and *FortiSandbox 4.0.0 VM Install Guide*.

Supported models

FortiSandbox version 4.0.0 supports the FSA-500F, FSA-1000F, FSA-1000F-DC, FSA-2000E, FSA-3000E, FSA-3000F, and FSA-VM (AWS, Azure, Hyper-V, KVM, and VMware ESXi) models.

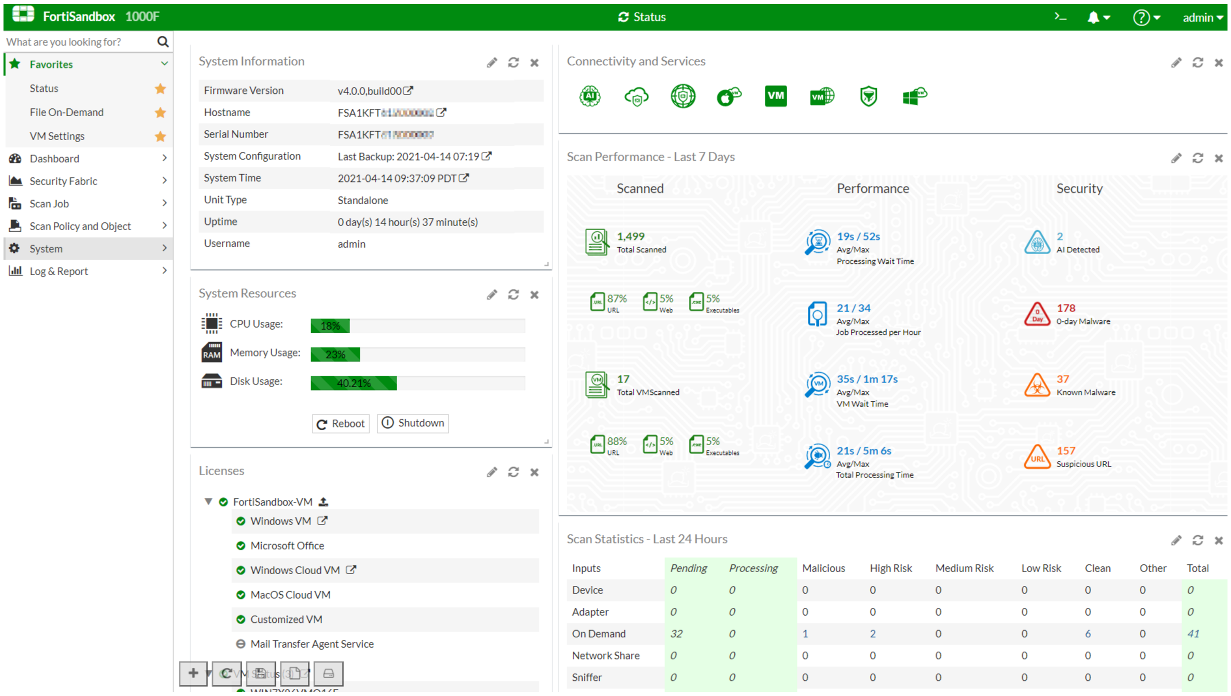
This version no longer supports FSA-1000D, FSA-3000D, FSA-3500D, and VM Base.

New features and enhancements

The following is summary of new features and enhancements in version 4.0.0. For details, see the *FortiSandbox4.0.0 Administration Guide* in the Fortinet Document Library.

GUI

- Redesigned menu layout and GUI Dashboard:
  - Implemented *Connectivity and Services* widget to show the operational status of the system.
  - Implemented *Scan Performance* widget to demonstrate the capabilities and capacity of the system.
  - Implemented *Licenses* widget to show the validity of contracts and services.
  - Implemented *System Resources* widget to show disk monitor information.
  - Implemented *Favorites* menu feature to customize and pick frequently used FortiSandbox features.



System Information

Firmware Version	v4.0.0,build00
Hostname	FSA1KFT[redacted]
Serial Number	FSA1KFT[redacted]
System Configuration	Last Backup: 2021-04-14 07:19
System Time	2021-04-14 09:37:09 PDT
Unit Type	Standalone
Uptime	0 day(s) 14 hour(s) 37 minute(s)
Username	admin

System Resources

CPU Usage: 18%

Memory Usage: 23%

Disk Usage: 40.21%

Scan Performance - Last 7 Days

Scanned	Performance	Security
1,499 Total Scanned	19s / 52s Avg/Max Processing Wait Time	2 AI Detected
87% URL, 5% Web, 5% Executables	21 / 34 Avg/Max Job Processed per Hour	178 0-day Malware
17 Total VMScanned	35s / 1m 17s Avg/Max VM Wait Time	37 Known Malware
88% URL, 5% Web, 5% Executables	21s / 5m 6s Avg/Max Total Processing Time	157 Suspicious URL

Scan Statistics - Last 24 Hours

Inputs	Pending	Processing	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	0	0	0	0	0	0	0	0	0
Adapter	0	0	0	0	0	0	0	0	0
On Demand	32	0	1	2	0	0	6	0	41
Network Share	0	0	0	0	0	0	0	0	0
Sniffer	0	0	0	0	0	0	0	0	0

- Introduced Cluster Management feature for administering HA-Cluster.
- Implemented reset of FortiGuard setting to default.
- Consolidated license upload of FSA-VM, Microsoft Windows, and Microsoft Office.
- Display a warning message before downloading any samples or malicious content from FortiSandbox.
- Display serial number or hostname if configured on the browser tab name.

Fabric integration

- Implemented custom VM support in a separate Virtual Private Cloud (VPC) in AWS platform.
- Implemented a separate port configuration for JSON REST API.
- Implemented hostname on HTTP connect in the request URI of FortiGuard proxy.
- Enhanced connectivity with FortiAnalyzer for secured logging.
- Enhanced LDAP related configuration via JSON RPC API to list all configurations and include advanced fields.

Scan

- Introduced new *Adaptive Scan Profile* feature that automatically adjusts the scan profile depending on the submission.
- Introduced VM Scan Ratio feature that is a new scan logic to balance the efficiency by utilizing the VMs based on system load.
- Introduced new dynamic scan module called PEXBox that emulates code for improved detection on Windows malware.
- Introduced new Rating Engine Plus feature that utilizes the cloud's rating.
- Implemented reset of prescan configuration back to default.
- Implemented deletion of VM Job while on Interactive Scan.
- Enhanced support on files with large filesize. Updated filesize limit and prescan CLI configuration.
- Improved scan behavior and rating on websites that are not 200 OK, for example, not reachable, forbidden, and so on.
- Improved scan flow for FortiMail Fabric Integration to return the result as soon as a known malware is detected.
- Set the AI mode enabled by default for higher detection rate.
- Implemented support for running multiple VM types at the same time for the same sample file or URL.

System & Security

- Introduced an alert system for system health check when a threshold is reached.
- Implemented FortiGuard as an available option for NTP server configuration.
- Implemented support for configuring cluster IP on aggregate interface for the bandwidth and redundancy of file submission.
- Implemented rescue mode feature on Hyper-V.
- Merged support for FortiSandbox 3000F model.
- Supported use of LACP interface on health check and MTA features.
- Updated filename of backup configuration from device serial number to hostname.
- Combined multiple rating engines for Windows, Android, and Linux into a single Sandbox Rating Engine.

Engines must be re-downloaded and might take several minutes. In HA-cluster, wait for each node to upgrade.

Logging & Reporting

- Redesigned PDF report to add more information of the job, including:
  - List of extracted URLs and VM images.
  - Signature info of antivirus detection.
  - Job details information on BCC feature.
  - Snapshot of system information and Engine/DB versions.
  - Configuration of AI, embedded URL option, scan timeout, and Windows Cloud VM region.
  - Reference link to VirusTotal reference.
- Implemented the Malware category field in the job event logs.
- Implemented detected malware name in the Suspicious Indicator Detail table.
- Implemented VM Category on the report as Default, Optional, or Custom.
- Implemented submit condition to VM Scan either by Scan Profile or new Scan Ratio; added to Job details report changes.
- Implemented logging of scan performance.

CLI

- Implemented CLI configuration for prescan module called `prescan-config`.
- Enhanced `tac-report` debug CLI command to include 4.0 features and to collectively run diagnose cli commands for monitoring and troubleshooting.
- Enhanced `test-network` debug CLI command to check network speed.
- Enhanced debug CLI command `test-network` to verify not only the cloud query but also cloud submission as part of the Community Cloud feature.
- Enhanced `status` CLI command to show the file system state of the boot and data disks.
- Display serial number or hostname if configured in the command prompt.
- Renamed `admin-pwd-reset` CLI command to `reset-admin-pwd`.

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 4.0.0 officially supports the following upgrade path.

Upgrade from	Upgrade to
3.2.0–3.2.2	4.0.0
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 > 4.0.0.

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 4.0.0 product integration and support information.

Web browsers	- Microsoft Edge version 89 - Mozilla Firefox version 87 - Google Chrome version 89 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	- 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	- 6.4.6 and later
FortiMail	- 6.4.0 and later - 6.2.0 and later - 6.0.0 and later - 5.4.0 and later
FortiClient	- 6.4.0 and later - 6.2.0 and later - 6.0.1 and later - 5.6.0 and later
FortiEMS	- 6.4.0 and later - 6.2.0 and later - 6.0.5 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
FortiProxy	- 7.0.0 - 2.0.0 and later - 1.2.3 and later

FortiWeb	• 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	• 6.00258
Tracer engine	• 4000.00009
System tool	• 4000.00084
Tracer sniffer	• 4000.00036
Virtualization environment	• VMware ESXi: 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.1 • KVM: Linux 4.15.0 qemu-img 2.5.0 • Microsoft Hyper-V: Windows server 2016 and 2019

Resolved Issues

The following issues have been fixed in FortiSandbox 4.0.0. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
673310	Fixed download report issue on Report Center when using Firefox.
690033	Fixed GUI logon using multi-factor authentication with FortiToken.
692145	Fixed loading of GUI pages on primary node of HA-Cluster when using Global Network.
690948	Fixed logon to the GUI with RADIUS 2-factor authentication.
693421	Fixed mouse movement issue when using VM Interaction mode.
648183	Improved loading response time of the *Job Details* page.
663459	Removed the *No valid software installed to support* in *VM Association* page to avoid confusion since those files are not executable in VM.

Fabric integration

Bug ID	Description
689623	Fixed connectivity issues with FortiClient that randomly gets stalled.
658449	Fixed package version number that displays incorrectly in FortiClient.
645576	Fixed RPC login issue when configured with LDAP wildcard.
688659	Improved the intermittent connection issue with the community cloud.

Scan

Bug ID	Description
681462	Enhanced the scan flow design to prevent premature job timeout.

Bug ID	Description
687843	Fixed a race condition when processing results from cluster nodes.
624697	Fixed clone number configuration issue that prevents adding more clones.
655346	Fixed decryption of files having cyrillic names causing detection loss.
653559	Fixed guest mouse pointer misalignment issue in Interactive mode.
666104	Fixed job verdict of parent URL when child URL is rated not clean.
682154	Fixed missing job details info due to retention policy discrepancies caused by heavy load.
696511	Fixed URL check function of the ICAP Adapter skipping the block listed URLs.
655941, 658574	Fixed NetShare scan stability.
686146	Fixed wrong behavior of handling YARA rules with *clean* risk level of 0 and 1.

System & Security

Bug ID	Description
662826	Fixed accepted version on TLS for GUI.
692151	Fixed high disk usage in FSA-VM environment.
681038	Fixed small footprint of memory leak on prescan daemon.

Logging & Reporting

Bug ID	Description
700168	Fixed sending SNMP trap when link is down on switch side.
690564	Fixed syslog format to include `host_id` after timestamp to conform to RFC.

Common vulnerabilities and exposures

Bug ID	Description
670283	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-22125
675152	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2020-29014
672978 672979	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-22124
680722	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-24010
680723	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-26097
672977	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2020-29011
675153	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-26096
683305	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-26098
680720 680785 680787 681362 681363 681364 681630 681633	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-24014
680721	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2020-29011
697271	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2021-24010
633086	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2020-15939
633044	FortiSandbox 4.0.0 is no longer vulnerable to the following CVE Reference: • CVE-2020-29012

Known Issues

The following issues have been identified in FortiSandbox 4.0.0. 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/restore.

FORTINET®

www.fortinet.com