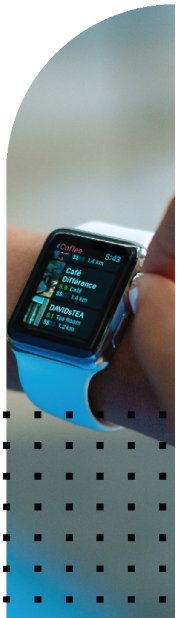
Release Notes

FortiSandbox 4.0.1



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/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

March 20, 2023
FortiSandbox 4.0.1 Release Notes
34-401-713667-20230320

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-09-02	Initial release.
2021-09-08	Updated Resolved Issues on page 14.
2021-10-06	Updated Resolved Issues on page 14.
2021-10-14	Updated Upgrade Information on page 9.
2021-11-02	Updated New features and enhancements on page 6.
2021-11-19	Updated Known Issues on page 16.
2023-03-20	Updated Upgrade Information on page 9.

Introduction

This document provides the following information for FortiSandbox version 4.0.1 build 0056.

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 4.0.1 Administration* and *Deployment Guides*.

Make sure to follow the upgrade path when upgrading your FortiSandbox device, particularly when upgrading an older device. For information, see Upgrade Information on page 9

New features and enhancements

The following is summary of new features and enhancements in version 4.0.1. For details, see the *FortiSandbox4.0.1 Administration Guide* in the Fortinet Document Library.

GUI

- Enhanced layout and usability of the *Scan Profile* web page.

Fabric integration

- Introduced the FortiAI integration support.

Scan

- Adjusted internal timeout value of the *VM Scan* to increase detection rate.
- Added *Parallel Scan* feature support on AWS and Azure.
- Adjusted behavior of *On-demand scan with Force* to run VM to continue even if sample is safelisted.
- Extended custom *Allow/Block* list with SHA256 to accept MD5sum and SHA1.

System & Security

- Introduced support for Custom-VM license as perpetual-based (previously, subscription-based).
- Added SNMP trap for contract/license expiration.

Logging & Reporting

- Improved communication to syslog server by enabling encryption.
- Added event log for system health-check.
- Improved rate and resilience of logging to FortiAnalyzer

CLI

- Added support to aggregate ip address via CLI.
- Added *Disk* and *Inode* usages on the response of get-system-status API.
- Provided new CLI command to cancel processing jobs.

Supported models

FortiSandbox version 4.0.1 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.

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 4.0.1 officially supports the following upgrade path.

Upgrade from	Upgrade to
4.0.0	4.0.1
3.2.4	Not Supported on 4.0.1 Upgrade to latest patch release of 4.0.
3.2.3	4.0.1
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, 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 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 4.0.1 product integration and support information.

Web browsers	• Microsoft Edge version 92 • Mozilla Firefox version 91 • Google Chrome version 91 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 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	• 7.0.0 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	• 7.0.0 and later • 6.4.6 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 • 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	• 6.2.0 • 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	• 6.4.0 • 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	• 6.00266
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 4.0.1. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
692145	Fix page loading error on FortiSandbox assigned as *Global Network Collector* due to unavailability of a contributor.
716553	In *VM interaction*, clicking the **x** button stops the scan process immediately.
716577	Fixed login failure with remote wildcard user which include character '@'.
729569	Fixed display error on *ICAP Adapter* web page.

Fabric integration

Bug ID	Description
689623	Fixed connectivity issues with FortiClient that randomly gets stalled.
726951	Fixed API response of UNKNOWN rating on zip file.

Scan

Bug ID	Description
708644	Fixed stuck issue on scanning *Network Share*.
713600	Fixed timeout issue when using *Parallel Scan* feature on *Custom RedHat VMs*.

System & Security

Bug ID	Description
711660	Fixed cluster upgrade timing issue when upgraded from older GA (e.g. 3.1) to 4.0.

Logging & Reporting

Bug ID	Description
694771	Fixed display issue of long and sub URL.

Common vulnerabilities and exposures

Bug ID	Description
672976	FortiSandbox 4.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2020-29013
684391	FortiSandbox 4.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2021-26105

Known Issues

The following issues have been identified in FortiSandbox 4.0.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

CLI

Bug ID	Description
731107	Incorrect disk usage on CLI of FortiSandbox in Azure.

Logging & Reporting

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

Scan

Bug ID	Description
716617	Timeout issue on Win10 VM clone due to a few incompatibility with Host's CPU.
728025	Improper use of URL whitelist on the Network Share scan.

System & Security

Bug ID	Description
575345	*Known Memory Yara* setting is not supported on *backup*/*restore*.
761582	Licensing issue after applying the perpetual-based Custom-VM license. (Request a special build from Support team for the fix).

www.fortinet.com