Release Notes

FortiSandbox 5.0.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 10, 2026
FortiSandbox 5.0.2 Release Notes
34-502-1147455-20260210

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
New features and enhancements **7**
Security Fabric & Deployment 7
Scan & Engine 7
GUI 7
Fabric Integration 8
System & Security 8
Logging & Reporting 8
CLI & API 8
Upgrade Information **9**
Before upgrade 9
Supported models 9
Downgrading to previous firmware versions 9
Firmware image checksums 9
Upgrade procedure 10
Upgrade path 10
Upgrade Notice 11
FortiSandbox 500G and 1500G models 11
FortiSandbox Hyper-V model 11
FortiSandbox GCP and OCI 11
Cluster environments 11
After upgrade 11
Tracer and Rating Engines 12
Android VM clones 12
Supported models 12
Product Integration and Support **13**
Special Notices **15**
GUI 15
Security Fabric 15
Scan & Engine 15
Resolved Issues **16**
CLI and API 16
Engine 16
Fabric integration 16
GUI 16
Logging & Reporting 17
Scan 17
System & Security 18
Common vulnerabilities and exposures 18

Known Issues **19**
System & Security 19

Change Log

Date	Change Description
2025-04-14	Initial release.
2025-05-07	Updated Known Issues on page 19.
2025-07-29	Updated Special Notices on page 15.
2025-07-29	Updated Resolved Issues on page 16.
2025-12-09	Updated Resolved Issues on page 16
2026-02-10	Updated Resolved Issues on page 16

Introduction

This document provides the following information for FortiSandbox version 5.0.2 build 0109.

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

New features and enhancements

The following is summary of new features and enhancements in version 5.0.2. For details, see the *FortiSandbox5.0.2 Administration Guide* in the Fortinet Document Library.

Security Fabric & Deployment

- Introduced a new Windows only license for simpler deployment of new OS.

Scan & Engine

- Introduced scanning support on SharePoint files.
- Introduced Windows 11 Custom VM.
- Enhanced secondary node of a cluster to be configured as standby without processing jobs.
- Added dynamic scanning of embedded URLs from QR codes.
- Added the option to keep the job folder on *Clean rating* (default is to delete job folder).
- Added support for long URL submissions through FortiMail.
- Added support to extract and scan PST files.
- Added support to extract URLs from *.eml* file from all input sources.
- Added support for downloading files from Google Drive.
- Added support for content type: *multipart/related*.
- Added setting custom rating for documents files feature.
- Added file-typing support on PS1 files.
- Released AI Engine 05000.00025 as GA on this patch release.

GUI

- Enhanced the GUI console with a complete redesign.
- Enhanced*Malware Package* page for better usability.
- Added support on importing IdP Metadata on the SAML SSO page.
- Added an option to delete multiple FortiGate and FortiClient devices in the *Security Fabric* page.

Fabric Integration

- Enhanced ICAP capability to support up to 1000 connections.
- Added a new configurable option to delete idle devices.

System & Security

- Introduced pooling and sharing of MTA seat count license on a HA cluster deployment.
- Introduced a new SKU for Windows activation only.
- Introduced FortiSandbox VMS as the new VM deployment model for both on premise and public cloud.
- Introduced a new CLI allowing user to change password with command line.
- Introduced integrated FortiSandbox PaaS into version 5.0.2.
- Enhanced job config protection to prevent malware detection evasion.
- Added secure connection to the FortiSandbox Community Cloud & Threat Intelligence.
- Added support for *root-OU* IAM account on FSA PaaS.
- Added support for profile assignment via SSO SAML assertion.
- Added HTTP support for community cloud query when proxy is used.

Logging & Reporting

- Enhanced *Job Details* page job report PDF to show all extracted URLs.
- Added Arabic filename support on the *Job Search* and *Details* pages.
- Added system event log when concurrent connection exceeds limit.
- Added a built-in default email server on PaaS for sending notifications email to user.

CLI & API

- Enhanced setup scripts for AndroidVMV5 VM to enhance stability.
- Added disk health in CLI hardware-info and tac-report, and SNMP.
- Added disk-usage CLI for disk usage on system, jobs and VMs.
- Added support for configuring customized VM ENA attribute installed from VHD file in AWS.

Upgrade Information

Before upgrade

Before any firmware upgrade, save a copy of your FortiSandbox configuration by going to *System* > *System Recovery*.

If you intend to use the new VMs after upgrade:

Ensure you have the appropriate VM licenses. Activating a VM requires the license specific to the version you are using with the equal number of clones. For example, if you have Win11 and Office 2021 activation keys you can use those keys to run the *Win11O21 VM*. If you want to configure 10 clones, then you will need 10 licenses.

Keep the following considerations in mind:

- We recommend purchasing a new license, downloading the VMs, and then reassigning the clones.
- If you download the new VMs (without updating your license) and then remove existing clones to make room for new ones, the old license will not work.

For more information about license keys, see *VM Settings > Optional VMs* in the *FortiSandbox Administration Guide*.

Supported models

FortiSandbox	FSA-500F, FSA-500G, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000E, and FSA-3000F
FortiSandbox-VM	ALI, AWS, Azure, GCP*, Hyper-V, KVM, Nutanix*, OCI* and VMware ESXi. *Although firmware images are available, test validation is conducted exclusively on the major General Availability (GA) release version.

For more information on VM, see the VM Installation Guide in the Fortinet Document Library.

Downgrading to previous firmware versions

Downgrading to previous firmware versions is not supported.

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*.

Upgrade procedure

When upgrading from 4.0.0 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 GUI, go to *Dashboard* > *Status*. Click in the *System Information* widget, and click *Update Firmware*. 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.

Upgrade path

FortiSandbox5.0.2 officially supports the following upgrade path.

Upgrade from	Upgrade to
5.0.0-5.0.1	5.0.2
4.4.7	5.0.0
4.4. 0 - 4.4.6	4.4.7
4.2.0 - 4.2.8	4.4.0
4.0.0 - 4.0.6	4.2.0

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 Notice

FortiSandbox 500G and 1500G models

For 500G and 1500G models, the upgrade path is *v4.2.5 NPI build* to *v4.4.3 build 0380* to v*4.4.6 build 0397* to *v5.0.0 build0073* to *v5.0.1 build0080*.

FortiSandbox Hyper-V model

1. Delete all checkpoints of the Virtual Machine instance that will be upgraded.
2. Power off the instance.
3. In Hyper-V Manager, go to navigating to the instance *Settings* > *IDE Controller* > *Hard Drive* > *Edit*. Increase the *fsa.vhdx* value to be larger than 1GB .

FortiSandbox GCP and OCI

The upgrade path on FortiSandbox GCP and OCI recommended by the GUI is not supported when upgrading from v4.2.3 to v4.2.4 and higher. As a workaround, you may upgrade directly to 4.4.0 GA, then follow the official upgrade path to 5.0.1 GA.

Cluster environments

Before upgrading, it is highly recommended that you set up a cluster IP set so the failover between primary and secondary can occur smoothly.

In a cluster environment, use this upgrade order:

1. Upgrade the workers and install the new rating and tracer engine. Then wait until the devices fully boot up.
2. Upgrade the secondary and install the new rating and tracer engine. Then wait until the device fully boots up.
3. Upgrade the primary. This causes HA failover.
4. Install the new rating and tracer engine on the old primary node. This node might take over as primary node.

After upgrade

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.

Rating engine

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.

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.

Android VM clones

Following the upgrade, any previously enabled Android VM clones will be disabled.

Supported models

FortiSandbox	FSA-500F, FSA-500G, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000E, and FSA-3000F
FortiSandbox-VM	ALI, AWS, Azure, GCP*, Hyper-V, KVM, Nutanix*, OCI* and VMware ESXi. *Although firmware images are available, test validation is conducted exclusively on the major General Availability (GA) release version.

For more information on VM, see the VM Installation Guide in the Fortinet Document Library.

Product Integration and Support

The following table lists FortiSandbox 5.0.2 product integration and support information. FortiSandbox integration and support is tested based on the firmware image of the product's latest available GA build during the release testing process. FortiSandbox also supports backwards compatibility to the product's earlier GA builds.

FortiSandbox integration and support is tested on the firmware image of the product's major release (*7.0.0, 7.2.0, 7.4.0* etc). Minor releases (*7.0.1, 7.0.2, 7.0.3* etc) are not individually tested because they are based on the same firmware image.

Where indicated, version *x.x.x and later* means integration and support is based on the major version, including minor versions unless otherwise indicated in the *Administration Guide* or *Release Notes*.

Android VM is not supported on FortiSandbox instances deployed on premise or public cloud, such as FSA VM, FSA Hyper-V VM, or FSA AWS, etc. However, the Android VM (AndroidVMV5) is supported on FortiSandbox hardware models.

Web browsers	• Google Chrome version 133 • Microsoft Edge version 134 • Mozilla Firefox version 136 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiManager	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiMail	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiClient	• 7.4.0 and later

	• 7.2.0 and later • 7.0.0 and later
FortiEMS	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiADC	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.2.0 and later • 6.1.0 and later
FortiProxy	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 2.0.0 and later
FortiWeb	• 7.6.0 and later • 7.4.0 and 7.4.1 • 7.2.0 and later • 7.0.0 and later
FortiIsolator	• 2.4.3 and later
FortiEDR	• 6.2.0 and later • 5.2.0 and later
AI engine (PAIX)	• 05000.00025
AV engine	• 00007.00037
FortiSandbox System tool	• 05000.00049
Traffic Sniffer Engine	• 00007.00183
Virtualization environment	• VMware ESXi: 5.1, 5.5, 6.0, 6.5, 6.7, 7.0.1 and 8.0 • KVM:Linux version 4.18.0 qemu-img v4.2.0 • Microsoft Hyper-V: Windows server 2016, 2019, and 2022 Hyper-V manager 10.0

Special Notices

GUI

The *Threats By Files*, *Devices*, *Hosts and Threats* dashboard pages have been deprecated as of v5.0.0.

The File, URL, Network Statistics, File Scan and URL Scan pages have been deprecated as of v5.0.0

Security Fabric

The Carbon Black adapter has been deprecated as of v5.0.0.

Scan & Engine

The Deep-AI and PEXbox engines have been deprecated as of v5.0.0 and replaced with the new *Advanced AI* engine.

The *Adaptive Scan* feature is no longer supported on the public cloud.

Several Web Categories are updated from Clean to Low Risk as of v4.4.0. Refer to *Web Category* for the updated list. When a job contains or links to a URL rated as Low Risk, then the job will be forwarded to the Dynamic VM Scan in order to check and possibly elevate the rating. However, this increases the jobs entering the VM. If the deployed system does not have the capacity to handle the increase, either override some categories to Clean as appropriate or increase selective categories to Medium Risk.

Resolved Issues

The following issues have been fixed in FortiSandbox 5.0.2. For inquiries about a particular bug, contact Customer Service & Support.

CLI and API

Bug ID	Description
1074215	Updated API 51 `set_admin_profile` by removing unnecessary fields.

Engine

Bug ID	Description

Fabric integration

Bug ID	Description
1137233	Fixed file submission issue via ICAP due to stale connections.

GUI

Bug ID	Description
987725	Fixed inaccurate error messages that were displayed when importing End Of Life OpenSSL PKCS12 Format CA.
1000605	Fixed error handling issue for Korean characters on the *LDAP Servers* page.
1092651	Fixed page filter issue of the *File Job* page after refresh.

Bug ID	Description
1098915	Fixed display issue in the *Job Report* for files with Arabic name submitted via ICAP proxy.
1108863	Fixed parameter validation on the scheduler query feature.
1114489	Added pop-up message box to prompt user to delete existing Android VM before install a new one
1119250	Fixed the broken link in the VirusTotal.
1132749	Removed AndroidV5 from the downloadable list for FortiSandbox VM deployments, including on-premise, public cloud, and PaaS.

Logging & Reporting

Bug ID	Description
1108590	Fixed event logging for both failed and successful login attempts via SNMPv3.
1117727	Fixed incomplete response for *usmStatsNotInTimeWindows* via SNMPv3.
1093987	Fixed order of the static and dynamic report sections.
1058220	Fixed missing *Behaviors In Sequence* section on job detail page of the PaaS platform.

Scan

Bug ID	Description
1121002	Fixed *Advanced AI* engine support on ICAP deployment.
1123171	Fixed FortiMail result issue caused by special characters in the URL.
1114102	Fixed scan result issue due to same file submission by multiple FortiMails.
1085073	Removed *In Cloud* icon from Incident Assist page due to slow loading
1105361	Fixed hot standby support of CustomVM in Public Cloud deployment with non nested mode.
1119536	Fixed scan logic of URL submission with payload via FortiMail.
1075404	Added compress file to the Sandbox package when a suspicious file is detected inside.
1123966	Fixed initialization and status issue of AndroidVMV5.

System & Security

Bug ID	Description
1047711	Fixed incorrect HDD status issue persisting after a PSU replacement.
1011934	Removed TLS1.1 support.
1117701	Fixed failed remote server backup to on Secondary and Worker nodes.
1100944	Disabled Cloud service checks on disabled features.
1115578	Fixed incorrect *Custom VM* count after upgrade to version 5.0.

Common vulnerabilities and exposures

Bug ID	Description
1129746	FortiSandbox 5.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2025-26466
1119938	FortiSandbox 5.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2025-52436

Known Issues

The following issues have been identified in FortiSandbox 5.0.2. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

System & Security

Bug ID	Description
1126263	Users experience slowness during FortiGuard database updates caused by jobs being rescanned.
1141918	FSA firmware can only support up to 96 CPU cores.

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.