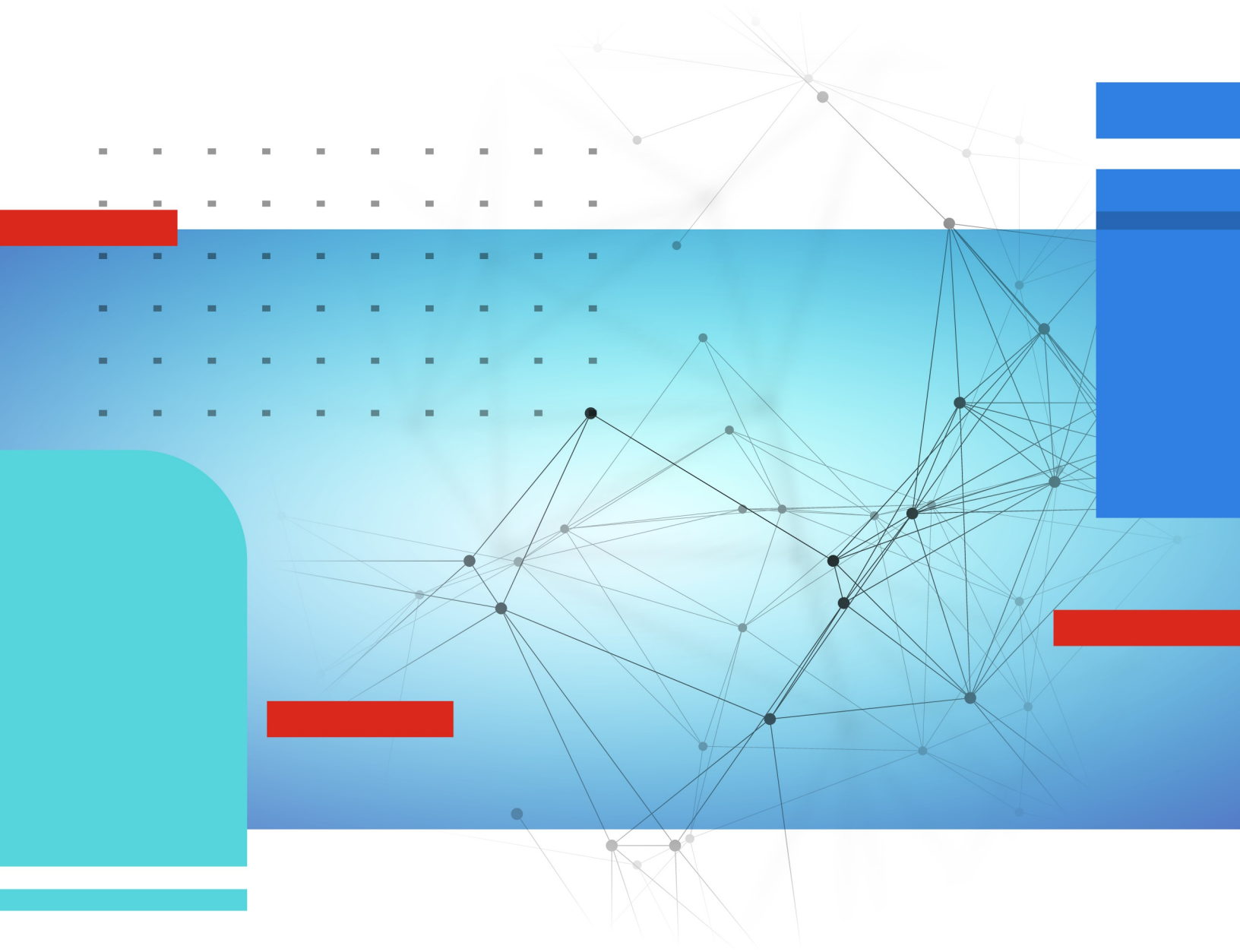
# Release Notes

## FortiSandbox 5.0.3



**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

December 10, 2025
FortiSandbox 5.0.3 Release Notes
34-503-1147469-20251210

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2025-08-13 | Initial release of version5.0.3. |
| 2025-08-19 | Updated Resolved Issues on page 15 and Known Issues on page 18. |
| 2025-08-20 | Updated Known Issues on page 18. |
| 2025-09-29 | Updated Resolved Issues on page 15. |
| 2025-12-09 | Updated Resolved Issues on page 15. |

# Introduction

This document provides the following information for FortiSandbox version 5.0.3 build 0133.

# New features and enhancements

The following is summary of new features and enhancements in version 5.0.3. For details, see the *FortiSandbox 5.0.3 Administration Guide* in the Fortinet Document Library.

## Scan & Engine

- Introduced a new scan mode called Lite Mode, designed for scanning large volumes of files primarily using static analysis. This mode supports essential Security Fabric integrations, NetShare, and only Pre-Filter policy configuration. In contrast, the default Full Mode includes both static and dynamic scanning, a complete set of deployment and integration options, and fully customizable policies.
- Introduced *Content Disarm and Reconstruction (CDR)* support for API and ICAP, enhancing security by sanitizing potentially malicious content from supported file types such as PDF and Microsoft Office documents.
- Enhanced the Log Server settings to include support for FortiAnalyzer Cloud.
- Enhanced manual PAIX package uploads by requiring a valid subscription.
- Enhanced the custom Linux VM to allow users to add and associate user-defined file extensions.
- Added an option to enable RTAP queries for URLs that are filtered out of Dynamic Scan.
- Added support for CAPTCHA recognition on web pages to the Real-Time Anti-Phishing service.
- Added URL Extraction from .msg file and scan the URLs.
- Added multiple file extractions in ICAP REQMOD.

## GUI

- Introduced *RTAP Statistics* to the *Dashboard*, allowing users to view threat detection data from RTAP service.
- Introduced browser selection support for FortiSandbox Cloud VMs.
- Enhanced the filters on the URL and File job pages, as well as the File and URL on-demand pages.
- Enhanced the VM Jobs page to allow users to adjust the size of the VM Job views as well as the ability to filter the displayed VM clones.
- Enhanced the Allow/Block list to support proper date format (e.g. %Y-%m-%d).
- Added a *Force dynamic scan on AV/Static detections* to the *Scan Profile > Advanced* tab.
- Added support for configuring the storage type when creating a customized FortiSandbox VM.

# Fabric Integration

- Introduced an option to use a proxy when sending password-protected encrypted files.
- Enhanced the *Inline Block Profile* to support more file types.

# Logging & Reporting

- Added an option to the *File On-Demand* settings that lets users specify which child files to scan within an archive.

# CLI & API

- Enhanced support for concurrent API connections.
- Added SSD operating status reporting to the tac-report CLI command.
- Added private link authentication on AWS.
- Added new options to the prescan-config CLI for configuring timeouts and limits based on file size during unpacking and YARA scanning.
- Added a new encryption option to the `format-storage` CLI for 3000G models.

# 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*.

For a list of supported hardware and VM models, see Supported models on page 11.

## 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 *Support > Downloads > 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

FortiSandbox5.0.3 officially supports the following upgrade path.

| Upgrade from | Upgrade to |
|---|---|
| 5.0.0 - 5.0.2 | 5.0.3* |
| 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 |

*FortiSandbox version 5.0.4 is now in GA release. Please consider upgrading to v5.0.4. For information, see the Release Notes.

**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

The upgrade path on FortiSandbox GCP 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, 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, 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.

# Supported models

| | |
|---|---|
| **FortiSandbox** | FSA-500F, FSA-500G, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000E, FSA-3000F and 3000G. |
| **FortiSandbox-VM** | AWS, Azure, GCP, Hyper-V, KVM, Nutanix and VMware ESXi. |

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

# Product Integration and Support

The following table lists FortiSandbox 5.0.3 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 137<br>• Microsoft Edge version 138<br>• Mozilla Firefox version 136<br>Other web browsers may function correctly but are not supported by Fortinet. |
| **FortiOS/FortiOS Carrier** | • 7.6.0 and later<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiAnalyzer** | • 7.6.0 and later<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiManager** | • 7.6.0 and later<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiMail** | • 7.6.0 and later<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiClient** | • 7.4.0 and later |

| | |
|---|---|
| | • 7.2.0 and later<br>• 7.0.0 and later |
| **FortiEMS** | • 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiADC** | • 8.0.0<br>• 7.6.0 and later<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later<br>• 6.2.0 and later<br>• 6.1.0 and later |
| **FortiProxy** | • 7.6.0 and later<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later<br>• 2.0.0 and later |
| **FortiWeb** | • 7.6.0 and later<br>• 7.4.0 and 7.4.1<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiIsolator** | • 3.0.0<br>• 2.4.3 and later |
| **FortiEDR** | • 6.2.0<br>• 5.2.0 and later |
| **AV engine** | • 00007.00045 |
| **FortiSandbox System tool** | • 05000.00062 |
| **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<br>• KVM: Linux version 4.18.0 qemu-img v4.2.0<br>• Microsoft Hyper-V: Windows server 2016, 2019, and 2022 Hyper-V manager 10.0<br>• Nutanix: AHV |

# 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 5.0.3. For inquiries about a particular bug, contact Customer Service & Support.

## CLI and API

| Bug ID | Description |
|---|---|
| 1147032 | Fixed the *Failed to stop watchdog and daemons* error that occurred when executing the *factory-reset* CLI command. |

## Fabric integration

| Bug ID | Description |
|---|---|
| 1181435 | Fixed an issue where customers were receiving an excessive number of "Verdict Notification Emails" for clean jobs. |

## GUI

| Bug ID | Description |
|---|---|
| 987725 | Fixed inaccurate error messages that were displayed when importing End Of Life OpenSSL PKCS12 Format CA. |
| 1158515 | Fixed an issue where Job Results (File Job, URL Job, and On-Demand options), and the Scan Statistics and Scan Performance widgets appeared empty. |
| 1180603 | Fixed an internal server error that occurred when accessing *System* > *FortiGuard*. |

# Logging & Reporting

| Bug ID | Description |
|---|---|
| 1137233 | Fixed a file submission issue via ICAP due to stale connections. |
| 1179548 | Fixed the packet capture CLI where syslog traffic sent from the port2 interface was incorrectly shown as using port1. |

# Scan

| Bug ID | Description |
|---|---|
| 1110864 | Resolved a mismatch in the Job Report behavior during scans that prevented incident analysis of a malicious file linked to a targeted phishing attack. |
| 1149471 | Fixed an issue with URL on-demand scans where FortiSandbox was truncating long URLs. |
| 1183391 | Fixed an issue where customized VMs failed to initialize on AWS non-nested instances. |

# System & Security

| But ID | Description |
|---|---|
| 1110346 | Fixed an issue where the data cleanup process removed job files but did not delete the empty folders. |
| 1141918 | FSA firmware can only support up to 96 CPU cores. |
| 1158431 | Fixed an issue where taking a large number of scan snapshots consumed excessive storage space. |
| 1166689 | Fixed the missing entries in the MIB file Description. |

# Common vulnerabilities and exposures

| Bug ID | Description |
|---|---|
| 1172018 | FortiSandbox 5.0.3 is no longer vulnerable to the following CVE Reference:<br>• CVE-2025-53679 |

| Bug ID | Description |
|---|---|
| 1172622 | FortiSandbox 5.0.3 is no longer vulnerable to the following CVE Reference:<br>• CVE-2025-53949 |
| 1172621 | FortiSandbox 5.0.3 is no longer vulnerable to the following CVE Reference:<br>• CVE-2025-54353 |

# Known Issues

The following issues have been identified in FortiSandbox 5.0.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

## Scan and Engine

| Bug ID | Description |
|---|---|
| 1191884 | Dynamic scan performance on FSA KVM VMs running FC4 with 128 CPUs is lower than on FC3 with 64 CPUs. |
| 1193238 | VM fails to initialize and enable due to a race condition with the firmware and engine upgrade. |

www.fortinet.com