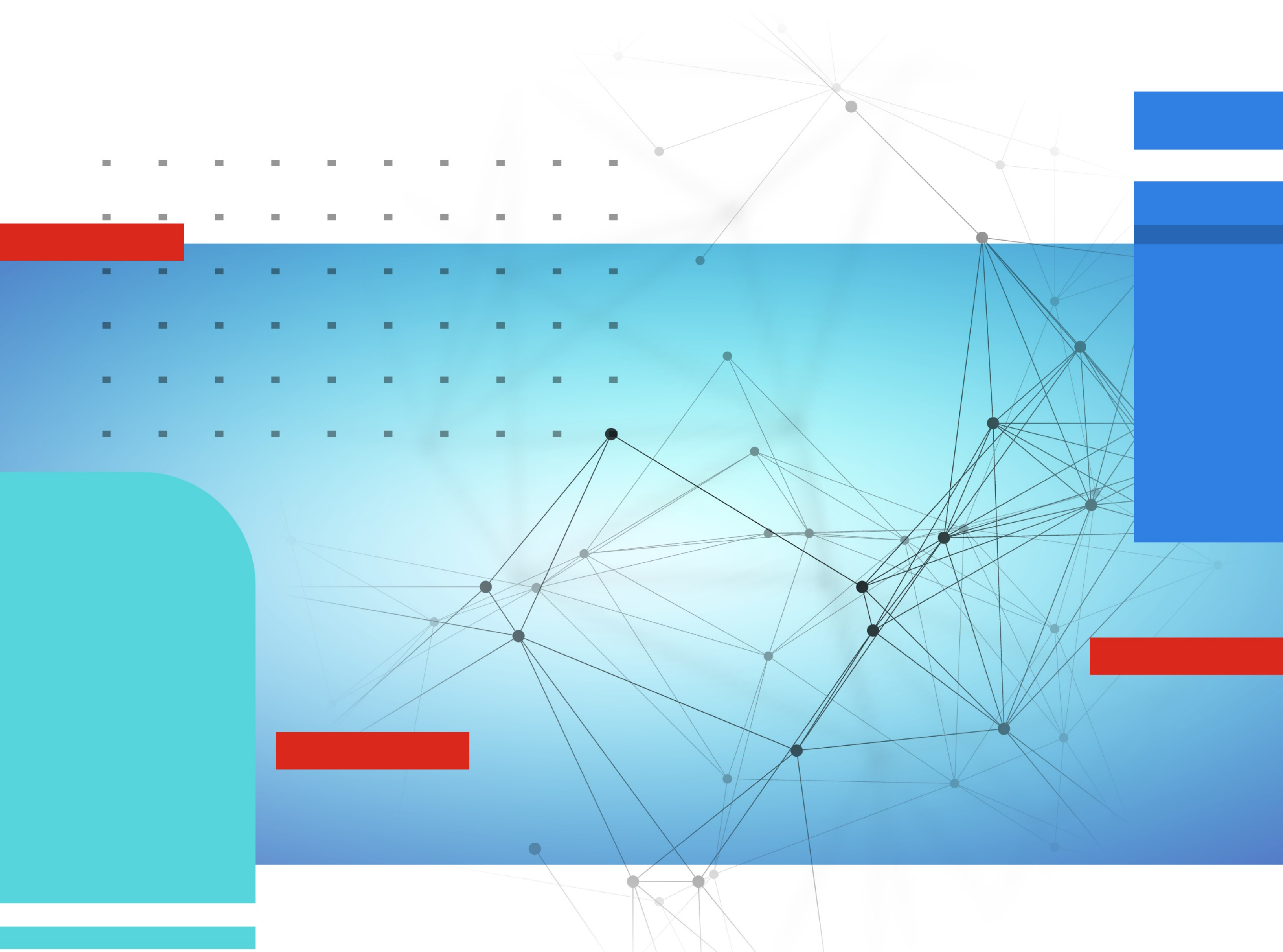
# Release Notes

## FortiSandbox 5.0.1



**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

September 29, 2025
FortiSandbox 5.0.1 Release Notes
34-501-1102546-20250929

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2024-12-18 | Initial release. |
| 2025-07-23 | Updated Resolved Issues on page 14. |
| 2025-07-29 | Updated Supported models on page 10. |
| 2025-09-29 | Updated Resolved Issues on page 14 |

# Introduction

This document provides the following information for FortiSandbox version 5.0.1 build 0080.

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

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 5.0.1 Administration Guide* and *FortiSandbox 5.0.1 VM Install Guide*.

# New features and enhancements

The following is summary of new features and enhancements in version 5.0.1. For details, see the *FortiSandbox5.0.1 Administration Guide* in the Fortinet Document Library.

## GUI

- Enhanced the Job Details report page with the following:
  - Static and Dynamic Analysis indicators labeled *Clean* are now labeled as *Info*.
  - Updated the icons of PDF and DOC files in the tree view
  - Sanitize the right-panel on tree-view details.

## Scan & Engine

- Introduced a pre-defined VM with Windows 11 IOT Enterprise LTSC with Office 2021 for AWS and Azure deployment.

# Upgrade Information

## Before upgrade

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

**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** | AWS, Azure, GCP, Hyper-V, KVM, Nutanix, VMware ESXi, GCP, OCI and VMware ESXi. |

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

FortiSandbox5.0.1 officially supports the following upgrade path.

| Upgrade from | Upgrade to |
|---|---|
| 5.0.0 | 5.0.1 |
| 4.4.6 | 5.0.0 |
| 4.4. 0 - 4.4.5 | 4.4.6 |
| 4.2.0 - 4.2.7 | 4.4.0 |
| 4.0.0 - 4.0.5 | 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 *v4.4.6 build 0397* to *v5.0.0 build0073* to *v5.0.1 build0080*.

## FortiSandbox PaaS

FortiSandbox PaaS is not supported by the main trunk. Please visit the FortiSandbox PaaS page for the latest upgrade information.

## 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 5.0.0 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.

# Supported models

| | |
|---|---|
| **FortiSandbox** | FSA-500F, FSA-500G, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000E, and FSA-3000F |
| **FortiSandbox-VM** | AWS, Azure, GCP*, Hyper-V, KVM, Nutanix*, VMware ESXi, GCP, OCI* and VMware ESXi.<br>*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 5.0.1 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*.

| | |
|---|---|
| **Web browsers** | • Google Chrome version 130<br>• Microsoft Edge version 129<br>• Mozilla Firefox version 130<br>Other web browsers may function correctly but are not supported by Fortinet. |
| **FortiOS/FortiOS Carrier** | • 7.6.0<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiAnalyzer** | • 7.6.0<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiManager** | • 7.6.0<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiMail** | • 7.6.0<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later<br>• 6.4.0 and later |
| **FortiClient** | • 7.4.0<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiEMS** | • 7.4.0<br>• 7.2.0 and later<br>• 7.0.0 and later |

| | |
|---|---|
| **FortiADC** | • 7.6.0<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<br>• 6.0.0 and later |
| **FortiProxy** | • 7.6.0<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<br>• 7.4.0 and 7.4.1<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiIsolator** | • 2.4.3 and later |
| **FortiEDR** | • 6.2.0 and later<br>• 5.2.0 and later |
| **AV engine** | • 00007.00030 |
| **FortiSandbox System tool** | • 05000.00039 |
| **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 4.15.0 qemu-img v2.5.0<br>• Microsoft Hyper-V: Windows server 2016, 2019, and 2022 |

# Special Notices

## GUI

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

The File, URL, Network Statistics, File Scan and URL Scan pages have been deprecated in 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 pf 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 5.0.1. For inquiries about a particular bug, contact Customer Service & Support.

## GUI

| Bug ID | Description |
|---|---|
| 987725 | Fixed inaccurate error messages that were displayed when importing End Of Life OpenSSL PKCS12 Format CA. |

## Fabric integration

| Bug ID | Description |
|---|---|
| 1097947 | Fixed a job processing stalled issue due to a mishandling of a compressed file with more than 4096 files. |

## Scan

| Bug ID | Description |
|---|---|
| 1096821 | Fixed an UNSEEN result issue on the FortiMail caused by a race condition during a change in FortiSandbox configurations. |

## System & Security

| Bug ID | Description |
|---|---|
| 1100314 | Fixed an empty customized VM name issue in the GUI that is caused by empty folders in the system. |
| 1091230 | Fixed an incompatibility issue on an unsupported custom VM based on Virtual Box v7.1 |

| Bug ID | Description |
|---|---|
| 1105493 | Fixed an activation issue on Office 2021 due to mishandling of key format. |
| 1097910 | Fixed a DB sync issue caused by UTF-8 characters in email subject. |

## Logging & Reporting

| Bug ID | Description |
|---|---|
| 1099505 | Fixed a job storage issue on temporary files related to URLs submitted through RPC. |

## Common vulnerabilities and exposures

| Bug ID | Description |
|---|---|
| 1055678 | FortiSandbox 5.0.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2024-3596 |

FORTINET®

www.fortinet.com

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.