Release Notes

FortiSandbox 5.0.5

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

January 29, 2026
FortiSandbox 5.0.5 Release Notes
34-505-1194108-20260129

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-11-06	Initial release of version 5.0.5.
2025-01-13	Updated Resolved Issues on page 15.
2026-01-29	Updated Supported models on page 10.

Introduction

This document provides the following information for FortiSandbox version 5.0.5 build 0141.

- Supported models
- New features and enhancements on page 6
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues on page 15

New features and enhancements

The following is summary of new features and enhancements in version 5.0.5. For details, see the *FortiSandbox 5.0.5 Administration Guide* in the Fortinet Document Library.

Scan & Engine

- Enhanced Inline Behavior processing by extending timeout to 180 seconds, allowing more time for analysis.

CLI & API

- Added support for the `ps-status` command on models previous to 3000E and 3000F.

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 10.

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

FortiSandbox5.0.5 officially supports the following upgrade path.

Upgrade from	Upgrade to
5.0.0 - 5.0.4	5.0.5
4.4.8	5.0.0
4.4.0 - 4.4.7	4.4.8
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, then follow the official upgrade path to 5.0.5.

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, then follow the official upgrade path to 5.0.5.

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 FSA-3000G.
FortiSandbox-VM	AWS, Azure, GCP, OCI, 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 5.0.5 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.

This minor patch addresses only one issue and, in line with our standard patch process, does not include full integration testing. Instead, we rely on the validation results from the previous release, where comprehensive testing was performed with the available builds at that time. Generally, newer patch releases of supported products maintain backward compatibility, and their integration can reasonably be assumed to function as expected. Repeating full integration testing across all products and versions for every minor update would introduce significant complexity and is not part of our regular patch workflow.

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 142 • Microsoft Edge version 142 • Mozilla Firefox version 144 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
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	• 8.0.0 and later • 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	• 8.0.0 and later • 7.6.0 and later • 7.4.0 and 7.4.1 • 7.2.0 and later • 7.0.0 and later
FortiIsolator	• 3.0.0 • 2.4.3 and later
FortiEDR	• 6.2.0 • 5.2.0 and later
AV engine	• 00007.00047
FortiSandbox System tool	• 05000.00071
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 • 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 5.0.5. For inquiries about a particular bug, contact Customer Service & Support.

Fabric integration

Bug ID	Description
1200763	Fixed an SSL handshake error between FortiSandbox and connected devices that occurred after upgrading to version 5.0.4

GUI

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

Logging & Reporting

Bug ID	Description
951647	Resolved an SNMP trap issue for link status changes caused by SNMP reboot behavior.
1199456	Fixed an issue where FSA failed to generate a threat activity report if a scanned URL exceeded 3K characters in length.

Scan and Engine

Bug ID	Description
1143279	Fixed an issue where FortiSandbox incorrectly treated corrupted Office files as ZIP archives.
1196525	Fixed RTAP query when in Air-gapped mode.
1201522	Fixed a malware package handling issue due to direct upgrade from FSA v5.0.0/5.0.1 to v5.0.4.

System & Security

But ID	Description
1196029	Resolved an issue where FSA-1000F units lost embedded Windows/Office licenses after upgrading to version 5.0.4.
1197642	Fixed an issue where hard-coded credentials were found in the login page.
1202816	Fixed the read-only privileges to prevent users from modifying system configurations by simulating valid requests.
1208169	Resolved an issue where the FortiSandbox inline block service exposed a private key.

Common vulnerabilities and exposures

Bug ID	Description
1199744	FortiSandbox 5.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2025-67685

www.fortinet.com