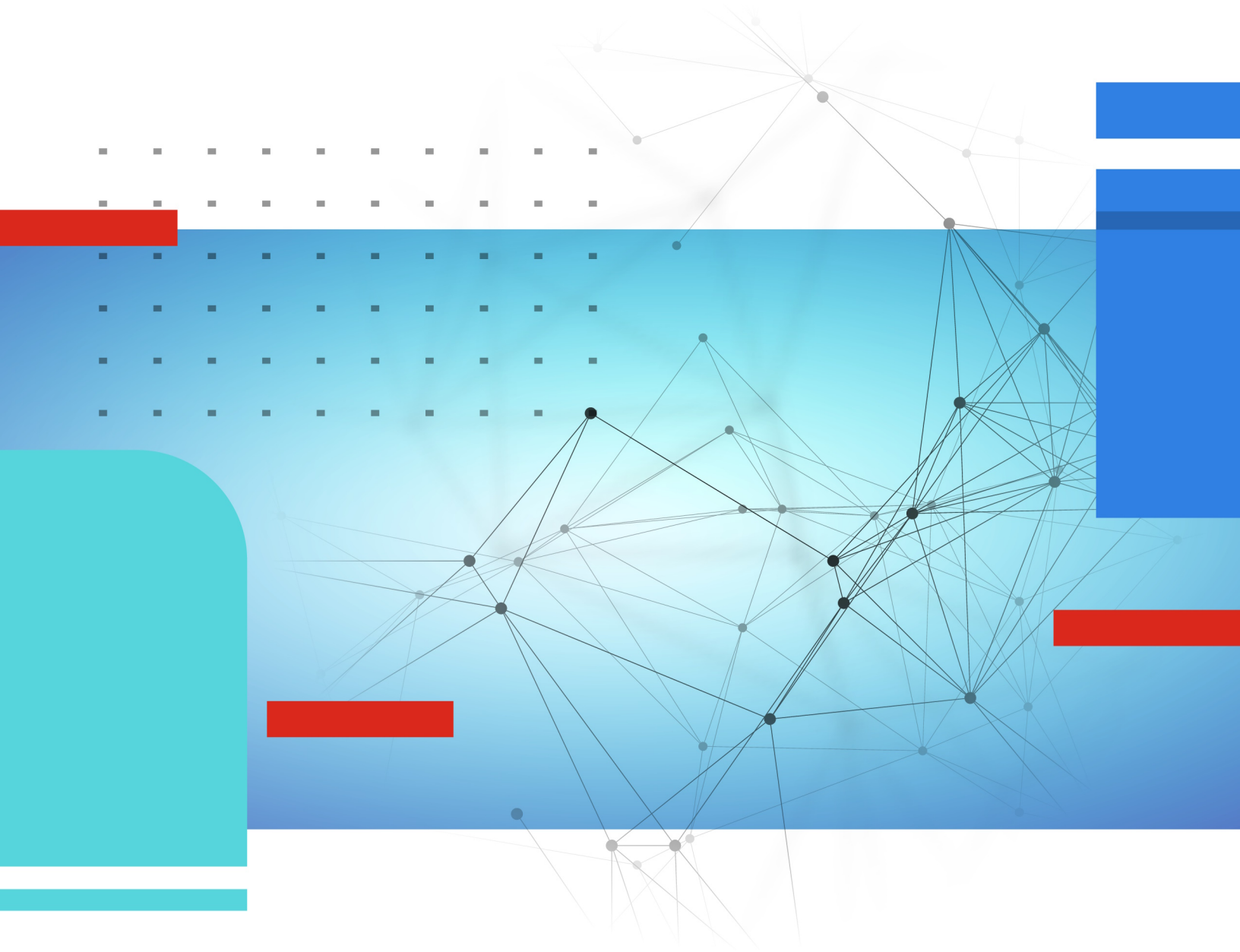
Release Notes

FortiSandbox 5.0.6



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

March 26, 2026
FortiSandbox 5.0.6 Release Notes
34-506-1250985-20260326

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-03-24	Initial release of version 5.0.6.
2026-03-26	Updated New features and enhancements on page 6.

Introduction

This document provides the following information for FortiSandbox version 5.0.6 build 0155.

New features and enhancements

The following is summary of new features and enhancements in version 5.0.6. For details, see the *FortiSandbox 5.0.6 Administration Guide* in the Fortinet Document Library.

Scan & Engine

- Introduced a re-scan mechanism for document files that automatically retries analysis when the associated application encounters unexpected crashes
- Enhanced sample-rating logic that allows FortiSandbox to accurately assess files hosted on trusted Fortinet domains, even when those domains are included in the default allowlist.
- Added a dedicated mode for cluster nodes that operate as primary or secondary members without performing any scanning functions.
- Added support for RHEL9 Custom VM deployments.

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

FortiSandbox5.0.6 officially supports the following upgrade path.

Upgrade from	Upgrade to
5.0.0 - 5.0.5	5.0.6
4.4.9	5.0.0
4.4.8	4.4.9
4.4.0 - 4.4.7	4.4.8

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 5.0.6.

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 5.0.6.

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	ALI, 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 5.0.6 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 145 • Microsoft Edge version 145 • Mozilla Firefox version 145 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
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiManager	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiMail	• 7.6.0 and later

	• 7.4.0 and later • 7.2.0 and later
FortiClient	• 7.4.0 and later • 7.2.0 and later
FortiEMS	• 7.4.0 and later • 7.2.0 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
FortiProxy	• 7.6.0 and later • 7.4.0 and later • 7.2.0 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 and later
FortiEDR	• 6.2.0 and later
AV engine	• 00007.00049
FortiSandbox System tool	• 05000.00080
Traffic Sniffer Engine	• 00007.01176
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 5.0.6. For inquiries about a particular bug, contact Customer Service & Support.

CLI and API

Bug ID	Description
1226626	Fixed the `show` command displaying member ports even after they were assigned to a bonded interface.
1230769	Fixed an issue where read-only LDAP accounts created through the CLI were unable to authenticate.

Fabric integration

Bug ID	Description
1224082	Fixed processing behavior problems in AWS ICAP Lite-mode (AV/Static-only).
1232093	Fixed the FortiSandbox Sniffer file-type selection so it now correctly restricts the types of files that are scanned.
1251141	Resolved an issue where the UI enforced a device serial-number pattern check for ILB deployments, preventing certain valid serial numbers from being accepted.
1257712	Fixed an issue where an air-gapped FortiSandbox appliance was initiating communication with public IP addresses.

GUI

Bug ID	Description
1192371	Updated the “Mexico City” timezone configuration so it correctly reflects Mexico’s elimination of Daylight Saving Time in 2023, ensuring DST is no longer applied.
1222229	Fixed a delay in displaying the file job log in a 1000F HA deployment when processing

Bug ID	Description
	files with long filenames.
1230241	Resolved an issue where the “Force dynamic scan on AV/Static detections” configuration option was being disabled after a system reboot.
1234003	Fixed the offline/online SNMP trap behavior on 1500G models.
1254533	Fixed an issue where uploading the AV package to the secondary unit failed with the error message “Allowed maximum size is 500 MBs.”

Logging & Reporting

Bug ID	Description
1232253	Resolved an issue where newly installed FSA-3000G units repeatedly generated the log message “SNMP_v3 Trap: Power 1 goes offline/online.”
1240484	Fixed an issue that caused the event log generation process to stop.

Scan and Engine

Bug ID	Description
1218631	Fixed an issue where the system was still querying the APT server when the remote Windows cloud VM was disabled.
1223409	Fixed an issue where database synchronization was delayed due to long filenames, resulting in an increased number of pending jobs.

System & Security

But ID	Description
1228856	Resolved an issue where OFTP on TCP 514 was flagged for weak TLS 1.2 RSA cipher suites.
1241106	Fixed an issue where the anti-phishing server list failed to update when FortiGuard traffic was routed through a proxy.

www.fortinet.com