Release Notes

FortiSandbox 4.0.3

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

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

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-03-16	Initial release.
2023-04-12	Updated Resolved Issues on page 12.

Introduction

This document provides the following information for FortiSandbox version 4.0.3 build 0084.

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

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 4.0.3 Administration Guide* and *FortiSandbox 4.0.3 VM Install Guide*.

Supported models

FortiSandbox version 4.0.3 supports the FSA-3000F, FSA-3000E, FSA-2000E, FSA-1000F-DC, FSA-1000F, FSA-500F, and FSA-VM (AWS, Azure, Hyper-V, KVM, and VMware ESXi) models.

> As of version 4.0.0., the following models are no longer supported: FSA-3500D, FSA-3000D, FSA-1000D, and VM Base.

New features and enhancements

This version contains bug fixes.

Upgrade Information

Before and after any firmware upgrade

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

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.

Upgrade path

FortiSandbox 4.0.3 officially supports the following upgrade path.

Upgrade from	Upgrade to	Notes
3.2.4 or 4.0.0-4.0.2	4.0.3	After upgrading a HA-Cluster from 4.0.0 or 4.0.1 to 4.0.2, re-configure the password for LDAP/RADIUS server on the new secondary node.
3.2.3	3.2.4	
3.2.0–3.2.2	3.2.3	
3.1.4	3.2.0	
3.0.6–3.1.3	3.1.4	
2.5.2–3.0.5	3.0.6	
2.4.1–2.5.1	2.5.2	
2.4.0	2.4.1	

> ⚠️ If you are using KVM or Hyper-V, the upgrade path must be 3.1.3 > 3.2.0, then follow the upgrade table.
> As with all VM upgrades, take a snapshot or make a checkpoint before upgrading.

> ⚠️ 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.

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.

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*.

Upgrading cluster environments

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

In a cluster environment, use this upgrade order:

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

Upgrade procedure

When upgrading from 3.1.0 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 Web UI, go to *System > Dashboard* . In the *System Information* widget, click the *Update* link next to *Firmware Version*. 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.

Downgrading to previous firmware versions

Downgrading to previous firmware versions is not supported.

FortiSandbox VM firmware

Fortinet provides FortiSandbox VM firmware images for VMware ESXi, Hyper-V, Nutanix, and Kernel Virtual Machine (KVM) virtualization environments.

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

Product Integration and Support

The following table lists FortiSandbox 4.0.3 product integration and support information.

Web browsers	• Microsoft Edge version 110 • Mozilla Firefox version 110 • Google Chrome version 110 Other web browsers may function correctly but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiAnalyzer	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later
FortiManager	• 7.0.0 and later • 6.4.6 and later • 6.2.1 and later • 6.0.0 and later • 5.6.0 and later
FortiMail	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.4.0 and later
FortiClient	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiClient EMS	• 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.5 and later
FortiADC	• 6.2.0 and later • 6.1.0 and later • 6.0.0 and later

	• 5.4.0 and later • 5.3.0 and later • 5.0.1 and later
FortiProxy	• 7.0.0 and later • 2.0.0 and later • 1.2.3 and later
FortiWeb	• 6.4.0 and later • 6.3.5 and later • 6.3.2 and later • 6.2.0 and later • 6.0.0 and later
AV engine	• 00006.00285
Tracer engine	• 4000.00009
YARA engine	• YARA engine I Version available upon request from Technical Support team.
System tool	• 04000.00106
Traffic sniffer	• 00004.00036
Virtualization environment	• VMware ESXi: 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.1. • KVM: Linux version 4.15.0 qemu-img v2.5.0 • Microsoft Hyper-V: Windows server 2019 and 2016

Resolved Issues

The following issues have been fixed in FortiSandbox 4.0.3. For inquiries about a particular bug, contact Customer Service & Support.

System & Security

Bug ID	Description
783889	Fixed gratuitous ARP issue on HA-cluster fail-back scenario.
889833	Supported FortiGate devices with only Fortinet CA2 certificate.

Bug ID	Description
795171	FortiSandbox4.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2022-27487

FÜRTINET

www.fortinet.com