FortiSandbox - Release Notes

Version 3.1.5

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

October 6, 2021
FortiSandbox 3.1.5 Release Notes
34-315-731218-20211006

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-29	Initial release.
2021-08-04	Updated Resolved Issues on page 10.
2021-09-08	Updated Resolved Issues on page 10.
2021-10-21	Updated Resolved Issues on page 10.

Introduction

This guide provides release information for FortiSandbox version 3.1.5 build 0147.

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.1.5 Administration Guide* and *FortiSandbox 3.1.5 VM Install Guide*.

Supported models

FortiSandbox version 3.1.5 supports the FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3500D, FSA-3000E, and FSA-VM (AWS, Azure, VMware ESXi, KVM, and Hyper-V) models.

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, clear the browser cache before logging in to the FortiSandbox to ensure the GUI displays properly.

Upgrade path

FortiSandbox 3.1.5 officially supports the following upgrade paths.

Upgrade from	Upgrade to
3.0.6–3.1.4	3.1.5
2.5.2–3.0.5	3.0.6
2.4.1–2.5.1	2.5.2
2.4.0	2.4.1

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

In a cluster environment, it is recommended to upgrade the cluster in the following order:

1. Worker devices
2. Secondary devices
3. Primary devices

Upgrade a unit after the previous one fully boots up. Before upgrading, it is highly recommended you set up a cluster level failover IP set, so the failover between Primary and Secondary devices can occur smoothly.

Upgrade procedure

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

As with all VM upgrades, take a snapshot or make a checkpoint before upgrading.

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

Firmware image for Hyper-V is not available due to upgrade issue specific to the Hyper-V environment.

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

Product Integration and Support

The following table lists FortiSandbox version 3.1.5 product integration and support information.

Web Browsers	• Microsoft Edge version 91 • Mozilla Firefox version 90 • Google Chrome version 91 Other web browsers may function correctly but are not supported by Fortinet.
FortiADC	• 6.0.0 • 5.4.0 and later • 5.3.0 and later • 5.0.1 and later
FortiAnalyzer	• 7.0.0 • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later
FortiClient	• 6.4.0 and later • 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiClient EMS	• 6.4.0 and later • 6.2.0 and later • 6.0.8 and later
FortiMail	• 7.0.0 • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.4.0 and later
FortiManager	• 7.0.1 • 6.4.0 and later • 6.2.1 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later
FortiOS/FortiOS Carrier	• 7.0.0 • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later

FortiProxy	• 1.2.3 and later
FortiWeb	• 6.3.2 and later • 6.2.0 and later • 6.0.0 and later • 5.8.0 and later
AV engine	• 6.00163
Tracer engine	• 3001.00153
Rating engine	• 3001.00063
System tool	• 3001.00584
Traffic Sniffer	• 00004.00036
Virtualization Environment	• VMware ESXi: 5.1, 5.5, 6.0, or 6.5 and later • KVM: Linux version 4.15.0 qemu v2.5.0 • Microsoft Hyper-V: Windows server 2016 and 2019

Resolved Issues

The following issues have been fixed in version 3.1.5. For inquiries about a particular bug, contact Customer Service & Support.

Logging & Reporting

Bug ID	Description
694771	Fixed display issue of long and sub URL.

Common vulnerabilities and exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
633086	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2020-15939
670283	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE-Reference: • CVE-2021-22125
672976	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2020-29013
672977	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2020-29011
675152	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE-Reference: • CVE-2020-29014
675153	FortiSandbox3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-26096
680720 680785 680787 681362 681363 681364 681630	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-24014

Bug ID	Description
681633	
680721	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2020-29011
680722	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-24010
680723	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-26097
683305	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-26098
697271	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-24010
672978 672979	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-22124
684391	FortiSandbox 3.1.5 is no longer vulnerable to the following CVE Reference: • CVE-2021-26105

Known Issues

The following issues have been identified in version 3.1.5. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Logging & Reporting

Bug ID	Description
578434	No confirmation ID in the log for the VM activation; resolved in FSA v3.2.0.

Scan

Bug ID	Description
561732	Upload to Community Cloud fails for AV rescan sample; resolved in FSA v3.2.0.

System & Security

Bug ID	Description
575345	Memory YARA setting is not supported on backup/restore.
577748	Network share configuration lost after upgrade from older GA release.
579978	Unprocessed alert setting is not supported on backup/restore.
581299	Cluster failed resync on config change from secondary (primary slave); Refer to updated Administration Guide for the proper way to resync.