FortiSandbox - Release Notes

Version 3.1.3

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 09, 2020
FortiSandbox 3.1.3 Release Notes
34-313-631794-20200609

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-06-09	Initial release.

Introduction and supported models

This guide provides release information for FortiSandbox version 3.1.3 build 0136.

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.1.3 Administration Guide* and *FortiSandbox 3.1.3 VM Install Guide*.

Supported models

FortiSandbox version 3.1.3 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.

New features or enhancements

The following is a list of new features and enhancements in version 3.1.3.

- The decompression tool for archive files has been enhanced to support Unicode filenames.
- The *Job Details* page has a new *No VM Reason* field.
- The `ping` command supports the continuous option.
- The `fw-upgrade` command supports the HTTPS protocol to download images.
- PDF reports support the Russian language.

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.

Upgrading to 3.1.3

FortiSandbox 3.1.3 officially supports upgrading directly from version 3.0.6, 3.1.0, 3.1.1, and 3.1.2.

To upgrade from other versions, see the following table.

Upgrading from	Upgrade path
3.0.0–3.0.5	3.0.0–3.0.5 > 3.0.6 > 3.1.3
2.5.0–2.5.1	2.5.0–2.5.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.3
2.4.0	2.4.0 > 2.4.1 > 3.0.0 > 3.0.6 > 3.1.3
2.3.0–2.3.2	2.3.0–2.3.2 > 2.3.3 > 2.4.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.3
2.2.1 or earlier	2.2.1 > 2.2.2 > 2.3.0 > 2.3.3 > 2.4.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.3

Upgrading cluster environments

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

1. Worker (slave) devices
2. Secondary (primary slave)
3. Primary (master)

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 (master) and secondary (primary slave) can occur smoothly.

Upgrade procedure

From 3.1.0 on, when new firmware is available, the Dashboard displays a blinking *New firmware available* link next to the *Firmware Version*. Click *New firmware available* to go to the *FortiSandbox Firmware Information* page where you can download and install firmware or manually upload new firmware.

To upgrade FortiSandbox firmware:

1. Download the firmware image from the Fortinet Customer Service & Support portal.
2. If upgrading using the GUI, go to *System* > *Dashboard* . In the *System Information* widget, click the *New firmware available* or *Update* link next to *Firmware Version*; then use the *FortiSandbox Firmware Information* or *Firmware Upgrade* page to upgrade the firmware.
3. If upgrading using the CLI, put the firmware image on a host that supports file copy with the SCP or FTP command. 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>
   ```
4. Microsoft Windows Sandbox VMs must be activated on the Microsoft activation server. 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.

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*.

Product Integration and Support

FortiSandbox 3.1.3 support

The following table lists FortiSandbox version 3.1.3 product integration and support information.

Web Browsers	• Microsoft Edge version 80 • Mozilla Firefox version 76 • Google Chrome version 80 Other web browsers may function correctly but are not supported by Fortinet.
FortiADC	• 5.4.0 and later • 5.3.0 and later • 5.0.1 and later
FortiAnalyzer	• 6.4.0 • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later
FortiClient	• 6.4.0 • 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiClient EMS	• 6.4.0 • 6.2.0 and later • 6.0.8 and later
FortiMail	• 6.4.0 • 6.2.0 and later • 6.0.0 and later • 5.4.0 and later
FortiManager	• 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	• 6.4.0 • 6.2.0 and later • 6.0.0 and later • 5.6.0 and later

FortiProxy	• 1.2.4
FortiWeb	• 6.3.2 • 6.2.0 and later • 6.0.0 and later • 5.8.0 and later
Virtualization Environment	• VMware ESXi: 5.1, 5.5, 6.0, or 6.5 and later • KVM: Linux version 4.15.0 qemu-img v2.5.0 • Microsoft Hyper-V: Windows server 2016

Resolved Issues

The following issues have been fixed in version 3.1.3. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
605918	Admin profile without privileged can access certain features.

Logging & Reporting

Bug ID	Description
514063	No log upon down interface.
518104	Encoding issue on the exported report.
577320	SNMP trap OID definition fsaTrapJobId not matching.
592097	PDF/CSV report generation fails due to special filename.
597491	No snmp trap on changing fsa mode to hc master.

Scan

Bug ID	Description
539668	Segmentation fault in the AV Engine.
594069	Prescan timed out on some particular files. Fixed on AV Engine.
594134	Upload white/black list with extra fields fails.
635699	On demand submission fails if through RPC API.

System & Security

Bug ID	Description
583447	Network share folder configuration fails to set password correctly.
583897	FortiManager as web filter server connection failure.
584257	Cluster failover synchronization issue of `set-tlsver` setting.
584772	GUI crash when adding Bit9 adapter.
588670	Cluster with dedicated primary (master) fails on fail over to standalone.

Bug ID	Description
592396	Quarantine mount failed with domain\username format.
606252	ICAP connectivity from SES Server as WAF not working.
622746	Stability issue on 3000E with very high load.

Known Issues

The following issues have been identified in version 3.1.3. 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.