FortiSandbox - Release Notes

Version 3.1.0

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 18, 2019
FortiSandbox 3.1.0 Release Notes
34-310-560233-20190618

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-06-18	Initial release.

Introduction

This document provides the following information for FortiSandbox version 3.1.0 build 0101:

- Supported models
- What's New in FortiSandbox 3.1.0
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.1.0 Administration Guide* and *FortiSandbox 3.1.0 VM Install Guide*.

Supported models

FortiSandbox version 3.1.0 supports the FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3500D, FSA-3000E, and FSA-VM (AWS, Azure, VMware ESXi and KVM) models.

What's New in FortiSandbox 3.1.0

Following is a list of new features in version 3.1.0:

- Auto notification for firmware upgrade.
- Support Linux VM and ELF file type scan.
- Improvement of *Job Detail* page.
- Newly designed On-Demand scan page.
- Allow users to toggle between AI mode scan and regular mode scan.
- Allow users to capture traffic of an interface for up-to 60 seconds.
- Support viewing details of non-Sandboxing job queue and purging it.
- Better management of device users with device group.
- Support wildcard admin authentication against remote LDAP and RADIUS user groups.
- Collect system kernel logs and CLI logs for troubleshooting.
- Support scan of AWS S3 bucket and Azure file share.
- Allow users to do an on-demand scan against a *Suspicious* jobs rated by static scan.
- Allow users to select an interface for the BCC adapter.
- Allow users to download VM images through a proxy server.
- French language support.
- A new indicator in the dashboard to show if the VM can download malicious payload through port3.
- Support Microsoft Azure platform.
- Support MTA for AWS platform.

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 prior to login on the FortiSandbox unit to ensure proper display of the web UI screens.

Upgrading to 3.1.0

FortiSandbox 3.1.0 officially supports upgrading directly from version 3.0.4.

- When upgrading from version 3.0.0 to 3.0.3, it is required to upgrade to 3.0.4 first, then to 3.1.0.
- When upgrading from version 2.5.0 to 2.5.1, it is required to upgrade to 2.5.2 first, then to 3.0.0 > 3.0.4 > 3.1.0.
- When upgrading from version 2.4.0, it is required to upgrade to 2.4.1 first, then to 3.0.0 > 3.0.4 > 3.1.0.
- When upgrading from version 2.3.0 to 2.3.2, it is required to upgrade to 2.3.3 first, then to 2.4.1 > 2.5.2 > 3.0.0 > 3.0.4 > 3.1.0.
- When upgrading from version 2.2.1 and earlier, the required upgrade path is as follows: 2.2.2 > 2.3.0 > 2.3.3 > 2.4.1 > 2.5.2 > 3.0.0 > 3.0.4 > 3.1.0.

Upgrading cluster environments

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

1. Slave devices
2. Primary Slave
3. Master

Upgrade a unit after the previous one fully boots up. After upgrade, it is highly recommended to setup a cluster level fail-over IP set, so the fail-over between Master and Primary Slave 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-based Manager, 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 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 3.1.0 support

The following table lists FortiSandbox version 3.1.0 product integration and support information.

Web Browsers	• Microsoft Edge version 44 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 66 • Google Chrome version 64 • Opera version 60 Other web browsers may function correctly, but are not supported by Fortinet.
FortiAnalyzer	• 6.2.0 and later (all FortiSandbox models) • 6.0.0 and later (all FortiSandbox models except FSA-500F/1000F) • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.8 and later
FortiADC	• 5.3.0 • 5.0.1 and later
FortiClient	• 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiEMS	• 6.0.5 and later • 6.2.0 and later
FortiMail	• 6.0.0 and later • 5.4.0 and later • 5.3.0 and later • 5.2.0 and later
FortiManager	• 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.8 and later
FortiOS/FortiOS Carrier	• 6.2.0 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later

	• 5.0.4 and later
FortiWeb	• 6.0.0 • 5.9.0 • 5.8.0 and later • 5.7.0 and later • 5.6.0 and later
Virtualization Environment	• VMware ESXi 5.1, 5.5, or 6.0 and later • KVM

Resolved Issues

The following issues have been fixed in version 3.1.0. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
502166	"Clean" rating results should not send to Syslog server when not enabled.
537563	Improve clone system stability and utilization.
539165	GUI *VM Status* page never times out.
539366	Not to extract archive files if they are from a whitelisted domain.
540246	DNS IP not assigned to custom VM.
540724	Members' VM list isn't synchronized to the HA Master if the global network scan profile management is enabled.
549134	Improve clone system stability and utilization.
549643	Website crashes when clicking on white/black list if it contains invalid characters.
550283	Android tracer engine update can cause Windows tracer engine to reset.
552115	Rewrite suspicious URLs inside PDF reports to improve security.
553908	Failed to upgrade packages through FDN because of missing certificates.
554450	Scan time-out when using Windows Cloud VM.
556025	Remove archive file types from *Scan Profile* and `sandboxing-prefilter` CLI command.
558615	On Demand specific file scan may start making another file and create high CPU usage by scanning these files
556963	Scheduled Networkshare scan jobs can't reach 100% on UI

Known Issues

The following are the known issues that have been identified in version 3.1.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Known issues

Bug ID	Description
537910	*Test Connectivity* from FortiGate 5.6.7 and 6.0.4 failed in HA mode FSA3500D and no jobs could be submitted.
543276	Resetting EMS file limitations affects other standalone FortiClients.
545018	FortiSandbox does not respond to FortiGate when FortiGate makes a connectivity test performed in the FOS GUI.
555409	Sometimes a network share cannot be deleted.
558929	GUI crashes due to Japanese characters in textbox files.
560417	Windows VM is not able to boot up on the OpenStack KVM platform.
560883	Scheduled PDF reports are deleted.
561382	FortiSandbox still responds to requests from FortiMail after FortiMail is unauthorized and deleted.
561758	Network share scan cannot be scheduled after job queue purge.
562010	*db-sync* process hangs up with a large amount of information in the *db-syn* folder.
563073	After restoring the configuration file, the unit is not in standalone mode.