FortiSandbox - Release Notes

Version 3.1.2

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

January 28, 2020
FortiSandbox 3.1.2 Release Notes
34-312-590252-20200128

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-10-23	Initial release.
2020-01-28	Deleted 578402 from Known Issues.

Introduction

This document provides the following information for FortiSandbox version 3.1.2 build 0124.

- Supported models
- What's New in FortiSandbox 3.1.2
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.1.2 Administration Guide* and *FortiSandbox 3.1.2 VM Install Guide*.

Supported models

FortiSandbox version 3.1.2 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.

What's New in FortiSandbox 3.1.2

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 prior to logging in to the FortiSandbox unit to ensure proper display of the web UI screens.

Upgrading to 3.1.2

FortiSandbox 3.1.2 officially supports upgrading directly from version 3.0.5, 3.1.0, and 3.1.1.

- When upgrading from version 3.0.0 to 3.0.4, it is required to upgrade to 3.0.5 first, then to 3.1.2.
- 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 > 3.0.5 > 3.1.2.
- When upgrading from version 2.4.0, it is required to upgrade to 2.4.1 first, then to 3.0.0 > 3.0.5 > 3.1.2.
- 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 > 3.0.5 > 3.1.2.
- When upgrading from version 2.2.1 and earlier, the required upgrade path is: 2.2.2 > 2.3.0 > 2.3.3 > 2.4.1 > 2.5.2 > 3.0.0 > 3.0.5 > 3.1.2.

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 failover IP set, so the failover between Master and Primary Slave can occur smoothly.

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.

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 3.1.2 support

The following table lists FortiSandbox version 3.1.2 product integration and support information.

Web Browsers	• Microsoft Edge version 44 • Mozilla Firefox version 68 • Google Chrome version 76 • Opera version 63 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 and later • 5.0.1 and later
FortiClient	• 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiEMS	• 6.2.0 and later • 6.0.5 and later
FortiMail	• 6.2.0 • 6.0.0 and later • 5.4.0 and later • 5.3.0 and later • 5.2.0 and later
FortiManager	• 6.2.1 and later • 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
FortiWeb	• 6.0.0 and later • 5.9.0 and later • 5.8.0 and later • 5.7.0 and later • 5.6.0 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 3.1.2. For inquiries about a particular bug, contact Customer Service & Support.

Resolved issues

Bug ID	Description
588329	The option “Force to Scan The file in VM" should be added to rescan windows.
589560	Inbound access through SSH and Telnet should be blocked for interface that is not enabled for them.

Known Issues

The following issues have been identified in version 3.1.2. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Bug ID	Description
561732	FortiSandbox cannot upload AV rescan sample to Community Cloud.
575345	Restored configuration did not restore memory yara.
577748	Network share configuration lost after upgrade if the netshare is created in a build older than 3.0.5.
578434	FortiSandbox does not give confirmation ID in the log.
579978	Configuration backup did not backup Unprocessed Alert setting.
581299	A restarted master should initially be a primary slave.
583569	Failed to test login for administrator with token authorization.
583897	Failed to connect FortiManager as web filter server.
584257	Failed to sync the setting of CLI `set-tlsver` in failover.
584772	Create new Bit9 Adapter caused GUI crash.