FORTINET
High Performance Network Security

FortiSandbox - Release Notes

VERSION 2.4.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

July 13, 2017

FortiSandbox 2.4.0 Release Notes

34-240-415859-20170713

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-05-03	Initial release.
2017-05-05	Added 374511 to *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2017-05-08	Updated *Upgrade Information* > *Upgrading to 2.4.0* upgrade paths.
2017-07-04	Added 405142 and 409891 to *Resolved Issues* > *Common Vulnerabilities and Exposures*.
2017-07-13	Added 408683 to *Resolved Issues* > *Common Vulnerabilities and Exposures*.

Introduction

This document provides the following information for FortiSandbox version 2.4.0 build 0252:

- Supported models
- What’s new in FortiSandbox 2.4.0
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 2.4.0 Administration Guide*.

Supported models

FortiSandbox version 2.4.0 supports the FSA-1000D, FSA-3000D, FSA-3500D, FSA-3000E, and FSA-VM (VMware ESXi, Citrix XenServer, and KVM) models.

What’s new in FortiSandbox 2.4.0

The following is a list of new features in version 2.4.0:

- Authorize FortiClient before accepting files
- Support On Demand scan video recording
- Support interact with VM for On Demand scans
- Support customized rating for Timeout and un-extractable archive files
- Support multiple file query in JSON RPC
- Allow users to enter a default password list for archive files
- Add per VDOM limitation for FortiGate file submissions
- Add SNMP trap when one power source fails
- Support centralized Malware and URL Package
- Support realtime AV scan for ICAP files
- Support reset widget
- Add ICAP block setting based on rating results
- Include white list in callback DB for files
- Support MacOS

The following is a list of enhancements in version 2.4.0:

- Improve UI usability
- Customized table columns
- VM screenshot available on the VM Status page
- Allow users to delete FP/FN verdicts

- Upload detected viruses to the Community Cloud
- Add tracer and rating engine versions in the Job Details page and report
- WINXP VM license is not supported due to Microsoft EOL
- Support Cloud Query by proxy

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 2.4.0

FortiSandbox 2.4.0 officially supports upgrading from version 2.3.3 to 2.4.0.

When upgrading from version 2.3.0 and 2.3.2, it is required to upgrade to 2.3.3 first, then to 2.4.0.

When upgrading from version 2.2.1 and below, the required upgrade path is: *2.2.2 > 2.3.0 > 2.3.3 > 2.4.0*.

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:

Step 1: Upgrade the firmware

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> - p<password> -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.

Step 2: Install Microsoft Windows VM package

If the unit does not have a Microsoft Windows VM package installed, they can be installed manually.

By default, FortiSandbox supports a base package of 4 Windows VM images.

To manually download the package:

1. **FSA-1000D, FSA-3000D, and FSA-VM models:**
   Download the package from ftp://fsavm.fortinet.net/images/v2.00/general_base.pkg
   FSA-3500D model:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/3500D_base.pkg

   FSA-3000E:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/3000E_base.pkg

   FSA-VM00:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/VM00_base.pkg

   Users can also purchase, download and install extra Android, Windows 8.1 and Windows 10 image packages. These packages can be downloaded from:

   Android:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/AndroidVM.pkg.7z

   Windows 8.1:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/WIN81VM.pkg.7z

   Windows 10:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/WIN10VM.pkg.7z

   MD5 File:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/md5.txt
2. Put the package 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.
3. In a console window, enter the following command string to download and install the package:

```
fw-upgrade -v -s<SCP/FTP server IP address> -u<user name> -p<password> -t<ftp|scp> -
    f<file path>
```

Step 3: Install the Microsoft Office license file

1. If the unit has no Office license file installed, download the Microsoft Office license file from the Fortinet Customer Service & Support portal.
2. Log into the FortiSandbox and go to *System > Dashboard* . In the *System Information* widget, click the *Upload License* link next to Microsoft Office. The *Microsoft Office License Upload* page is displayed. Browse to the license file on the management computer and select the *Submit* button. The system will reboot.
3. The Microsoft Office license must be activated against the Microsoft activation server. This is done automatically after a system reboot. To ensure the activation is successful, port3 must be able to access the Internet and the DNS servers should be able to resolve the Microsoft activation servers.

For FSA-3000D and FSA-1000D specific models, contact Fortinet Customer Service & Support to obtain the license file.

Step 4: Install Windows 8.1 or Windows 10 license files

1. If user purchases Windows 8.1 or Windows 10 support, download the Windows license file from the Fortinet Customer Service & Support portal
2. Log into FortiSandbox and go to *System > Dashboard*. In the *System Information* widget, click the *Upload License* link next to *Windows VM* field. The *Microsoft VM License Upload* page is displayed. *Browse* to the license file on the management computer and click the *Submit* button. The system will reboot.
3. The Microsoft Windows license must be activated against the Microsoft activation server. This is done automatically after a system reboot. To ensure the activation is successful, port3 must be able to access the Internet and the DNS servers should be able to resolve the Microsoft activation servers. Network configurations for port3 can be configure on the *Scan Policy > General* page.

Step 5: Check system settings

After upgrading, from a version prior to 2.2.0, the following settings should be checked in order for system to work as expected

1. Check *Network > System Routing* page and *Network > System DNS* page to make sure the static routing and DNS settings are correct for non-guest VM traffic. As port3 is reserved for guest VM traffic, all existing static routings on port3 should be removed.
2. Check *Scan Policy > General* to make sure the next hop Gateway, proxy server and DNS settings are correct for guest VM images to communicate externally.
3. Check *Virtual Machine > VM Images* page to make sure the clone number of each VM type is expected.
4. Check *Scan Policy > Scan Profile* page to make sure each file type is scanned by the correct VM type.
5. Go to *Scan Policy > URL Category* page to make sure the checked URL categories should be excluded from the malicious list.
6. Go to *Log & Report > Log Servers* to make sure the log servers are receiving expected levels of logs.

When upgrading from a previous release, the database will be rebuilt. The *Database Not Ready* message will be displayed on web pages.
The rebuild time depends on the existing data volume.

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, Citrix XenServer, and Kernel Virtual Machine (KVM) virtualization environments.

More detailed information can be found in the VM Installation Guide, which is available on 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 Checksum*s, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiSandbox 2.4.0 support

The following table lists FortiSandbox version 2.4.0 product integration and support information.

Web Browsers	• Microsoft Internet Explorer versions 10 and 11 • Mozilla Firefox version 32 • Google Chrome version 36 Other web browsers may function correctly, but are not supported by Fortinet.
FortiAnalyzer	• 5.0.8 and later • 5.2.0 and later • 5.4.0 and later
FortiClient	• 5.4.0 and later
FortiMail	• 5.2.0 and later
FortiManager	• 5.0.8 and later • 5.2.0 and later • 5.4.0 and later
FortiOS/FortiOS Carrier	• 5.0.4 and later • 5.2.0 and later • 5.4.0 and later • 5.6.0
FortiWeb	• 5.4.0 and later
Virtualization Environment	• VMware ESXi 5.1, 5.5, or 6.0 and later • Citrix XenServer 6.5 and later • KVM

Resolved Issues

The following issues have been fixed in version 2.4.0. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
391026	Timezone Turkey, Istanbul GMT +3 end of Daylight Saving (DST).
396089	FSA-VM serial number may be overwritten after performing a config restore.
396094	AVDB last update time gets changed whenever there is a FSA power cycle.
398665	`reports.py` may crash if too many files are scheduled in the PDF report.
402366	Return most recent rating to ICAP client.
402593	Returned ICAP URL rating is incorrect if there is a different rating for a file from the URL.
402800	Should list the latest logs on the top in *Network Share* scan details.
403175	REST API does not accept files with diacritic characters in the name.
403420	*FortiView Threats by Host* search may not work.
403910	Sniffer widget may crash.
404433	File submissions from FortiWeb are reported as *failed submitted files*.
405263	May not be able to delete a remote admin containing special characters.
405485	Device status shows *Up* status even if it is not connected.
407690	`CTRL-C` closes the SSH session .
408065	ICAP Receive File function does not work.
411031	No URL result returned to FortiMail .
414635	Daemon may be crashed when FortiMail submits a long URL.
414968	Trace can not support French Version of Windows.

Bug ID	Description
415533	FCT `src-ip` and `dst-ip` may be reversed.
400854 401170	Support F5 ASM and other reverse proxy vendors using different ICAP file submission command.

Common Vulnerabilities and Exposures

Bug ID	Description
374511	FortiSandbox 2.4.0 is no longer vulnerable to the following CVE-References: • 2016-2847 • 2016-2546 • 2016-2545 • 2016-2544 • 2016-2384 • 2016-0723 • 2015-7515 • 2015-1339 Visit https://fortiguard.com/psirt for more information.
405142	FortiSandbox2.4.0 is no longer vulnerable to the following CVE-References: • 2017-3731 • 2017-3730 • 2017-3732 • 2016-7055 Visit https://fortiguard.com/psirt for more information.
408683	FortiSandbox2.4.0 is no longer vulnerable to the following CVE-References: • 2016-2183 Visit https://fortiguard.com/psirt for more information.
409891	FortiSandbox2.4.0 is no longer vulnerable to the following CVE-References: • 2017-6214 Visit https://fortiguard.com/psirt for more information.

Known Issues

There following are the known issues that have been identified in version 2.4.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Known issues

Bug ID	Description
402208	URL maybe rated as *High Risk* when its behavior has just one Low Risk entry.
406229	Less processing jobs than enabled clone numbers
410672	FortiSandbox in *Sniffer Mode Scan* is not able to recognize files transmitted via SMB protocol with Chinese characters
414892	Can not filter Malware/URL package by *SN* and *Global/Local*.
415700	Network share does not support detailed link in *Threat by Topology* page.
417740	Manual AV-rescan result may not be correct when sample is in `extreme-db`.
421360	Primary slave may not prompt itself to Master after master changes to standalone mode.

FORTINET

High Performance Network Security