FortiSandbox - Release Notes

VERSION 2.5.0

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

December 15, 2017

FortiSandbox 2.5.0 Release Notes

34-250-449301-20171215

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Supported models 5
What's new in FortiSandbox 2.5.0 5
Upgrade Information **7**
Before and after any firmware upgrade 7
Upgrading to 2.5.0 7
Upgrading Cluster Environments 7
Upgrade procedure 7
Step 1: Upgrade the firmware 8
Step 2: Install Microsoft Windows VM package 8
Step 3: Install the Microsoft Office license file 9
Step 4: Install Windows 8.1 or Windows 10 license files 9
Step 5: Check system settings 9
Downgrading to previous firmware versions 10
FortiSandbox VM firmware 10
Firmware image checksums 10
Product Integration and Support **11**
FortiSandbox 2.5.0 support 11
Resolved Issues **12**
Known Issues **14**

Change Log

Date	Change Description
2017-11-02	Initial release.
2017-11-07	Added a note regarding read or device level privileges in *Upgrade Information* > *Upgrading to 2.5.0*.
2017-11-08	Added 458544 to *Known Issues*.
2017-11-20	Added 459700 and 459335 to *Known Issues*. Updated *Product Integration & Support* > *FortiAnalyzer*.
2017-12-15	Removed Citrix XenServer support from *Upgrade Information* > *FortiSandbox VM Firmware*.

Introduction

This document provides the following information for FortiSandbox version 2.5.0 build 0320:

- Supported models
- What's new in FortiSandbox 2.5.0
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 2.5.0 Administration Guide*.

Supported models

FortiSandbox version 2.5.0 supports the FSA-1000D, FSA-2000E, FSA-3000D, FSA-3500D, FSA-3000E, and FSA-VM (VMware ESXi and KVM) models.

What's new in FortiSandbox 2.5.0

The following is a list of new features in version 2.5.0:

- Support job queue priority adjustment
- Added rescue boot partition
- Display samples detected by FortiGate on the Operation Center page
- Search for AV rescan jobs in Log and File Detection page
- Included suspicious URLs (only depth=0) in URL Package
- Added On-Demand scan results in Malware Package
- Added Read/Write/None permission settings to Admin Profiles
- Added CLI command to rebuild RAID
- Added Calendar View of major events
- Support multiple network share scan jobs priority
- Support user defined extensions in sniffer setting
- Support password locked file for Office and PDF files from FortiEmail
- Seat count support for MACOS file scans
- Added Skip the job scan after timeout feature for files received from FortiMail
- Support *hash* library in Yara engine
- Provided JSON RPC API to download original file and PDF report
- Share MACOS licenses among cluster nodes

The following is a list of enhancements in version 2.5.0:

- Added CLI commands to specify SSL versions
- Added CLI commands to disable the maintainer user
- Do not send un-subscription URLs to VM
- Added warning message for customized VM clone#
- Added ramdisk and memory usage
- Hide debug tracer log in job details
- Added CLI command to reset tracer/rating engine to base
- Included detailed behaviors in its PDF report if from job detail page
- Added VM disk usage on dashboard
- Added option to generate STIX file without behaviors
- Added option to include jobs with clean rating on remote log server setting
- Included time zone within the timestamp of the detailed report

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 2.5.0

FortiSandbox 2.5.0 officially supports upgrading from version 2.3.3, 2.4.0, and 2.4.1 to 2.5.0.

When upgrading from version 2.3.0 and 2.3.2, it is required to upgrade to 2.3.3 first, then to 2.5.0.

When upgrading from version 2.2.1 and below, the required upgrade path is: *2.2.2* > *2.3.0* > *2.3.3* > *2.5.0*.

After upgrading to v2.5.0, admin users with *read* or *device* level privilege will match to the default admin profile *Read Only* or *Device*. By default, those two admin profiles do not have the *Download original file* and *JSON API* permissions enabled . Users need to manually add them back if needed.

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-BASE models:**
   Download the package from ftp://fsavm.fortinet.net/images/v2.00/general_base.pkg

   FSA-2000E model:

   Download the package from ftp://fsavm.fortinet.net/images/v2.00/2000E_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 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 2.5.0 support

The following table lists FortiSandbox version 2.5.0 product integration and support information.

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 54 • Google Chrome version 59 Other web browsers may function correctly, but are not supported by Fortinet.
FortiAnalyzer	• 5.6.1
FortiClient	• 5.4.0 and later • 5.6.0 **Note**:Starting from FSA 2.5, FCT 5.6.0 and below devices will be automatically authorized.
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 and later
FortiWeb	• 5.4.0 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 2.5.0. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
417740	Manual AV-rescan result is not correct when sample is in `extremedb`.
418009	Eicar Downloader is rated as clean by MAC OS scan.
418229	Malware Package STIX report is not correct.
424279	Job Archive creates truncated file names if it contains a column character.
436118	*Download Original Files* returns 500/404 errors when the filename contains unreadable characters.
436434	FortiSandbox does not check the link of a long spam URL..
436478	File still executed in VM when file type is disassociated from the Scan.
436482	Malware/URL package should not contain Global Iformation if FortiSandbox is in Local mode.
437068	`sandboxing-prefilter trustvendor` option does not sync between HC members.
437293	Should not use `sandbox-cached` rating for a new job after enabling `embedded-url`.
437921	Incorrect Email subject displayed in log.
438136	Processing URL jobs from sniffer are not shown on the Dashboard.
438978	FP on clean .xls and .pdf and word files after upgrading to 2.4.1.
439039	Job Detail page should display office scanner static rating behavior.
439417	Anti-Sandbox Evasion sample is not detected.
441540	In Fortiview, the *Special Characters Found* filename is displayed.
444312	Customized Rating for password-protected file is not working.

Bug ID	Description
444519	Video link should be protected by login.
444648	URL search does not work on the FortiView-URL Scan Search page.
445743	Job are rated as unknown without a VM scan retry.
402208	URL is rated as High Risk even its behavior has just one Low Risk entry.
452882	Forti Sandbox should only provide verdicts not the scanned file back to ICAP client.

Known Issues

There following are the known issues that have been identified in version 2.5.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Known issues

Bug ID	Description
454457	FortiClient authorized icon may not reflect the real status.
454808	Read only user may still able to submit jobs for rescan.
455413	Submission from FortiClient registered to FortiGate may not count as a FortiClient submission.
455591	Issue when deleting admin profiles.
455844	`executing cleandb` may yield unrelated message on console.
456195	FortiClient's hostname is displayed as *N/A* after upgrade if it does not send files.
457063	You many not be able to edit Admin Profile using Internet Explorer.
458544	*admin* users may lose CLI or GUI access after upgrading in HC mode. **Workaround:** For GUI access issue: In the GUI go to *System* > *Administrators* page, assign a proper admin profile to users. For CLI access issue: Create a new admin profile, assign it to the user, and apply the setting. Then, assign the original profile to the user and apply the setting.
459700	Domains not being protected by FE may be listed as a device. **Workaround:** Uncheck *New VDOMs/Domains Inherit Authorization* on FortMail , and de-authorize any unwanted FE domains listed in the device list.
459335	The default admin user's untrusted hosts setting is disabled.

FORTINET

High Performance Network Security