FORTINET
High Performance Network Security

FortiSandbox - Release Notes

VERSION 2.3.3

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

January 31, 2017

FortiSandbox 2.3.3 Release Notes

34-233-399350-20170131

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Supported models 5
What's new in FortiSandbox 2.3.3 5
Special Notices **6**
FortiSandbox 3000E Port Labelling 6
Upgrade Information **7**
Before and after any firmware upgrade 7
Upgrading to 2.3.3 7
Upgrading Cluster Environments 7
Upgrade procedure 7
Step 1: Upgrade the firmware 7
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 2.3.3 support 11
Resolved Issues **12**
Known Issues **15**

Change Log

Date	Change Description
2017-01-19	Initial release.
2017-01-20	Added *CVE References* to *Resolved Issues* > *Common Vulnerabilities and Exposures* section.
2017-01-26	Added *404433* to *Known Issues*.
2017-01-31	Added *Special Notices* > *FortiSandbox 3000E Port Labelling*. Added *405009* to *Known Issues*.

Introduction

This document provides the following information for FortiSandbox version 2.3.3 build 0205:

- Supported models
- What's new in FortiSandbox 2.3.3
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 2.3.3 Administration Guide*.

Supported models

FortiSandbox version 2.3.3 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 2.3.3

The following is a list of new features and enhancements in version 2.3.3:

- Allow user to disable Community Cloud Query
- Allow user to remove an entry/entries from Malware Packages
- Allow user to generate PDF reports in *FortiView>Threats by Devices* at first and second levels
- Allow user to add comments when submitting a job by On-Demand
- Allow user to disable the AV rescan
- Allow user to apply one YARA rule to multiple file types
- Allow user to export YARA rules
- Added Threat Timeline Chart in *Threats by Files* and *Threats by Devices* pages
- Added a centralized page to show manually marked FP/FN jobs
- Added CLI commands to set port3 gateway and DNS
- VM00 model 2 support
- Malware/URL packages moved to *Scan Policy* > *Package Options*.
- Improved OFTPD performance
- When resources cannot handle enabled clone # a warning message will appear for FSA-VM models
- Show quarantined jobs in Network Share scan result page

Special Notices

FortiSandbox 3000E Port Labelling

FortiSandbox 3000E units with a serial number in the following ranges have their port 5 and port 6 reversed. The ports on the back of the unit from left to right should read 6 and 5.

- FSA3KE3R16000039 and less
- FSA3KE3R17000014 and less

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 2.3.3

FortiSandbox version 2.3.3 officially supports upgrading from version 2.2.2, 2.3.0 and 2.3.2.

When upgrading from version 2.2.1 and below, it is recommended to upgrade to 2.2.2 first, then to 2.3.3.

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 is not does not have 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/general/image/2.0.0/2015022118_vm.pkg.7z

   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 2.3.3 support

The following table lists FortiSandbox version 2.3.3 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
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 2.3.3. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
385320	Job Summary page on Master unit shows inaccurate slave nodes job count.
394219	Finished percentages is displays 100% after a Network Share scan starts.
393685	Master sometimes cannot retrieve data from slave node.
391928	For FSA-3500D, RAID information is removed from the Disk Monitor widget.
393888	Maximum URL settings in *Scan Profile* page is not applied.
394727	The last row cannot be viewed when scrolling vertically in the *System* > *Administrators* page
387730	Rated by value cannot be sent to the Community Cloud if the result is not from Community Cloud Query.
395300	Between the CLI and the Web UI, there is a discrepancy of the SIMNET status.
390867	Reduce Health Check interval limit with a ping server.
396877	JSON API `get_jobs_of_submission` always returns `0` jobs when queried with a `sid`.
397253	File count is wrong when FGT device name contains special characters.
397543	Some malware is not included in the Malware Package.
397259	Job counts in the *Scan Input* > *Device* page are not accurate.
397251	Files may not enter Sandboxing if Cloud Query has errors.
394762	WIN7X86VM stops working if the clone # is 1.
396812	Malware Package did not check the Whitelist.
398973	URL scan issue if Weblink is not associated with any VM types.

Bug ID	Description
398158	URL category is not shown in reports.
398863	Malware type should not be displayed as *N/A* in report and page.
399452	*File Detection* > *Summary Report* page does not display Adapter data correctly.
399309	On-Demand filter returns empty result when Search by Device is On Demand.
397652	MS word files timeout after 15 min if embedded-URL enabled.
398504	FSA cannot use Fortigate SOCK5 proxy for FortiGuard services.
397212	FDN Service Status is not consistent between GUI and the test network.
395979	Failed to find corresponding VM for job.
393858	Sandbox VM system does not work as expected.
398965	FSA-VM returns *Core module exited for VM recovery* message often.
400146	VM system is re-initialized at the fourth scan profile update.
399272	Authentication to network share fails if password contains a special character.
389910	Unable to scan Network Share if the share path contains a special character.
398697	Re-scan shows different results.
389910	Unable to perform Network Share scan if file path has special characters.
399294	*Database not available* error message is displayed when viewing scan statistics if the load is heavy.
400691	Only 50 jobs are listed on URL On-Demand second level page.
402189	`win7x64vm` is not activated on XenServer 6.5.
402197	Segmentation does not work as expected when generating a large PDF report.
402282	More than expected jobs are pending when the Pre-scan times out.
402423	Cannot submit 100M files from FortiMail.

Common Vulnerabilities and Exposures

Bug ID	Description
382338	FortiSandbox 2.3.3 is no longer vulnerable to the following CVE-References: • 2016-6308 • 2016-6307 • 2016-6306 • 2016-6305 • 2016-6304 • 2016-6303 • 2016-6302 • 2016-2183 • 2016-2182 • 2016-2181 • 2016-2179 • 2016-2178 • 2016-2177 Visit https://fortiguard.com/psirt for more information.

Known Issues

There following are the known issues that have been identified in version 2.3.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Known issues

Bug ID	Description
387537	File name in Unicode may not show correctly.
395124	If there is Japanese in the file name may cause GUI internal server error.
398665	`reports.py` may crash if too many files are in scheduled PDF report.
396089	FSA-VM serial number may be overwritten after performing a `config restore`.
400212	Clean URLs may be rated as *High Risk* by Customized VM.
400854	Dashboard/FortiView/Search maybe inoperable under heavy load.
403175	REST API may not accept files with diacritic characters in the file name.
403298	Searching long file names containing special characters may return empty in the Search results or in the PDF report.
403420	*FortiView Threats by Host* search may not work.
404433	You may not be able to submit FortiWeb files.
405009	SFP+ port 5 and 6 label are reversed. The ports on the back of the unit from left to right should read 6 and 5. Please see Special Notices on page 6.

FORTINET®

High Performance Network Security