FortiSandbox Release Notes

VERSION 2.1.2

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 17, 2015

FortiSandbox 2.1.2 Release Notes

34-212-302561-20151217

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-12-17	Initial release.

Introduction

This document provides the following information for FortiSandbox version 2.1.2 build 0105:

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 2.0 Administration Guide*.

Supported models

FortiSandbox version 2.1.2 supports the FSA-1000D, FSA-3000D, FSA-3500D, and FSA-VM models.

What's new in FortiSandbox 2.1.2

The following is a list of new features and enhancements in version 2.1.2:

New Feature	Description
Centralized Management of Slave nodes on the Master node in a Cluster	Users can perform any of the following tasks to a Slave node on a Master node in a Clustering environment: **a.** View the Slave node's dashboard. **b.** Switch the Slave node's role using the Dashboard > System Information widget. **c.** Configure the Slave node's network settings (IP address, routing table, DNS and Proxy settings). **d.** Upgrade the Slave node (firmware, AV, database, etc.). **e.** View the Slave node's VM status page. Change made: *System* > *HA Cluster*

New Feature	Description
Improved FortiMail and FortiClient support	FortiMail Email metadata information is displayed in the Job Detail page. **a.** Email Sender **b.** Email Receiver **c.** Email Sender's IP **d.** Email Subject URLS from FortiMail will be scanned and the results can be checked. For FortiClient. login user of host, host's hostname, and IP address are sent over by FortiClient and displayed Change made: (*Job Detail* > *File-based Detection* > *File Input* > *FortiClient* > *URL detection*).
Allow user to adjust the scan power of the Master node in a Cluster	In a Clustering environment, the user can adjust the Master node's scan power by percentage. Change made: (`hc-master` CLI command).
Improved device bootup speed	System bootup speed increased by more than 100%.
Improved system performance in Cluster Mode	Fast job dispatch and job data collection.
Allow user to define White and Black listed domains	Users can define White or Black listed domain names for a file's downloaded URL. If the domain name of the downloaded URL matches the White or Black List, the file can be rated as Malicious or Clean immediately. Change made: (*Config* > *White List and Config* > *Black List*).
Allow use to search historical logs in the Local Log page	Log files on FortiSandbox are rotating and by default only current ones are used for searching. Users can search historical log files if needed. Change made: (*Log & Report* > *Log* > *Local Log*)
Report generation cancellation support	Users can cancel report generation if it takes too long. Change made: *Job Data* > *Export Data*

Upgrade Information

Upgrading from FortiSandbox 1.4.0 or later

FortiSandbox version 2.1.2 supports upgrading from version 1.4.0 or later.

Upgrading from FortiSandbox 1.3.0

FortiSandbox version 2.1.2 does not support upgrading from version 1.3.0.

Upgrading from FortiSandbox 1.2.3

FortiSandbox version 2.1.2 does not support upgrading from version 1.2.3.

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/<filename>
   ```
3. When upgrading via the Web-based Manager, go to *System* > *Dashboard* > *Status*. 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 the new Microsoft Windows VM package

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

To manually download the package:

1. For 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

   For the FSA-3500D model, download the package from ftp://fsavm.fortinet.net/3500D/image/2.1.0/vm.pkg.7z
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<filename>
```

To automatically download the package:

1. FortiSandbox version 2.0 has a background program which can automatically check for and download new Microsoft Windows VM packages. The system must be able to access https://fsavm.fortinet.net.
2. After log in, select *System* > *Dashboard* > *Status*. In the *System Information* widget, a progress bar will be displayed beside the Windows VM row to display the download progress.
3. When the download is complete, the dashboard will display an *Install New* link. Click the link and confirm to install the package.
4. Microsoft Windows Sandbox VMs 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.

Step 3: Install the Microsoft Office license file

1. For the FSA-VM model, download the Microsoft Office license file from the Fortinet Customer Service & Support portal.
2. Log into the FortiSandbox and go to *System* > *Dashboard* > *Status*. 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.

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 (5.5 and up) virtualization environments:

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiSandbox VM installation.
- `.ovf.zip`: Download the 64-bit package for a new FortiSandbox VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

When deploying FortiSandbox VM, the virtual disk size should be 150GB or more. 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 2.1.2 support

The following table lists FortiSandbox version 2.1.2 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
FortiClient	• 5.4.0 and later
FortiMail	• 5.2.0 and later
FortiManager	• 5.0.8 and later • 5.2.0 and later
FortiOS/FortiOS Carrier	• 5.0.4 and later • 5.2.0 and later
FortiWeb	• 5.4.0 and later
Virtualization Environment	• VMware ESXi version 5.5 and later

Resolved Issues

The following issues have been fixed in version 2.1.2. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
297077	Processing job count is not accurate in Scan Statistics widget in the Dashboard.
297417	The URL Scan Job detail page does not load the Behavior Chronology Chart.
267462	Patch CVE-2015-0235 GHOST vulnerability.
296969	CLI command `cleandb` does not work as expected.
297772 298099	CLI command `factory-reset` does not work as expected.
298317	CLI command `pending-jobs-purge` does not work as expected.
298332	When FortiMail submits a URL to scan, use the Email's session ID as the filename to trace back to the original email.
297083	Total malware count in Alert Email is not accurate.
294725	Sniffed files are not put in the job queue in Cluster mode.
298108	One virus file should be re-scanned by the AV only once.
295115	Clean/Unknown jobs should be removed from the second page of Threats by Device page.
297699	Device information is wrong in the second page of the Threats by Device page.
299174	Local Log search should not be case sensitive.
297714	File count is not accurate in first page of the Threats by Device page.
289181	Network share scan result does not always appear.

Bug ID	Description
296254	When deleting a network share, a disk I/O error occurs.
296828	In Cluster mode, the finished percentage might not show as 100% even if the scan finishes.
297219	Error message about the JS engine shows up in console.
296694	Slave node applies the synchronized configuration unnecessarily.
293789	Remove Rescan Rating field in the printed report if the job is not a rescan job.
297273	Job dispatcher crashes when Master node dispatches media files to Slave node.
297512	In Job detail page, the Code Emulation section name is changed to Static Analysis.
289336	Excel file is incorrectly executed by Microsoft Word in the VM.
299879	Device name is duplicated in the Device page.
300095	Improve job clean up performance.
299773	Fix rating false positives.
300197	In job detail page of a URL scan job, Submit Type is wrong if the URL is from FortiMail.
299872	The web server keeps restarting after IPV6 is set on Port1.
299342	Support new file types, like MSI files and Outlook msg files.
300087	Remove Malicious rating information for URL scans.
300639	Hide Office software from the Scan Profile if it is not activated.
297245	Hide the Log menu for a read-only user.
300620	In Job Detail page, the Digital Signature information is incorrect.
301285	The device status is always up in Device page even though there is no traffic from it.
297560	An error occurs when decompressing the second level of a .tar file.
301314	An error occurs when building a URL package for a device.

Bug ID	Description
301984	After rebooting FSA, the FortiSandbox Engine package goes back to the original one.
300649	YARA rules are not applied for certain file types.
302176	Filtering error in *Device* > *URL Package* page
297045	Uploading AV database package form FortiCare website does not work.
302274	Allow primary slave to use 100% of power to do scan.
298450	*URL Detection* > *Summary Report* widgets show incorrect data.
300759	In the Job Detail page, the Infected OS information is missing.
299608	Improve session management for RPC sessions.
300596	Return the static scan result to the RPC user when the job detail information is queried.
297048	The web page does not respond immediately after uploading the Sandbox Engine package.
302739	Deadlock can occur when the frequency of the job result query is high.
302742	An error can occur when generating or sending a scheduled summary report for a device.

Known Issues

The following issues have been identified in version 2.1.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Known issues

Bug ID	Description
245008	The unicode file name might not display correctly.
296643	Some network behaviors may not be displayed in the *Chronology Chart* and *Behavior In Sequence* section of the Job Detail page.