FortiSandbox Release Notes

VERSION 2.1.1

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

October 20, 2015

FortiSandbox 2.1.1 Release Notes

34-211-296644-20151020

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-10-20	Initial release.

Introduction

This document provides the following information for FortiSandbox version 2.1.1 build 0095:

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

Supported models

FortiSandbox version 2.1.1 supports the FSA-1000D, FSA-3000D, and FSA-VM models.

What's new in FortiSandbox 2.1.1

The following is a list of new features and enhancements in version 2.1.1:

- Added Behavior Chronology Chart in the Job Detail page
- Applied a new style to the PDF version of the job detail report
- Allow users to choose VM types to scan EXE files from the Scan Profile page
- Added support to overwrite Scan Profile settings during On-Demand scans
- Allow users to input passwords to extract archive files during On-Demand scans
- Allow users to input password protected PKCS12 Certificate
- Scan script file types like .js, .bat, .vbs, .ps1, .cmd files
- Allow user to receive a notification email when a suspicious verdict is retrieved by a client device
- Scan embedded URLs inside document files and PDF files
- Allow users to integrate third party Yara rules
- Added Login Disclaimer
- Read-only LDAP and RADIUS users support
- Allow users to schedule report generation
- Device VDOM level email alert and report support
- Improved Sniffer setting page
- Drill-down of Summary Report widgets support
- All device models are allowed to work as cluster Master or Primary Slave node

Upgrade Information

Upgrading from FortiSandbox 1.4.0 or later

FortiSandbox version 2.1.1 supports upgrading from version 1.4.0 or later.

Upgrading from FortiSandbox 1.3.0

FortiSandbox version 2.1.1 does not support upgrading from version 1.3.0.

Upgrading from FortiSandbox 1.2.3

FortiSandbox version 2.1.1 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. 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

The Microsoft Windows VM package can be installed manually or automatically.

To manually download the package:

1. Download the package from ftp://fsavm.fortinet.net/general/image/2.0.0/2015022118_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 100GB or more.

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 2.1.1 support

The following table lists FortiSandbox version 2.1.1 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

Resolved Issues

The following issues have been fixed in version 2.1.1. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
295202	Total file count is not correct for archive files in the On-Demand page when the scan is in-progress.
294291	Imported certificate can not be applied after reboot.
293830	In the dashboard, the processing number is not accurate.
293811	Job destination IP is not correct when performing a pattern search in the *FortiView* > *Search* page.
294725	Sniffed files are not put in the job queue in Cluster mode.
288824	HTTP server does not start up when changing the certificate.
285635	Cannot view the Screen Shot in the Job Detail page.
285463	The `NAS IP` in the *RADIUS Server configuration* is sent in reverse order during authentication.

Known Issues

The following issues have been identified in version 2.1.1. 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.