FORTINET
High Performance Network Security

FortiSandbox - Release Notes

VERSION 2.2.1

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

July 20, 2016

FortiSandbox 2.2.1 Release Notes

34-221-372046-20160720

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-05-26	Initial release.
2016-07-20	Added FSA-3500D to Supported Models.

Introduction

This document provides the following information for FortiSandbox version 2.2.1 build 0148:

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 2.2.0 Administration Guide*.

Supported models

FortiSandbox version 2.2.1 supports the FSA-1000D, FSA-3000D, FSA-3500D, and FSA-VM models.

What's new in FortiSandbox 2.2.1

The following is a list of new features and enhancements in version 2.2.1:

New Feature	Description
Allow user to build and upload their own customized Windows XP and Windows 7 images	User can create their own customized guest VM images and upload them to FortiSandbox for scans. Changes made: 1. CLI command `vm-customized` to upload customized image . 2. *Virtual Machine* > *VM Images* page has a special section to display customized images.
A new FortiView page which shows detected malware and their status	The page displays 0-day malware (caught before AV signature is available). It also shows if the malware is included in generated dynamic malware package and if it is uploaded to FortiSandbox Community Cloud. User can also mark what actions he/she has taken to respond to the incident. Changes made: *FortiView* > *Operation Center* .
Allow user to easily download and install Fortinet published guest VM images	User can view, download and install newly published VM images by Fortinet. Changes made: *Virtual Machine* > *VM Images* .

New Feature	Description
Support domain name in the wildcard format in White Domain List and Black Domain List	User can specify an `*.` in front of a domain name to match all its sub-domains.
Allow user to scan a single URL through On-Demand	User can scan a URL directly instead of saving it to a file first. Changes made: *Scan Input* > *URL On-Demand* .
Allow user to skip static scan result when job is submitted through On-Demand or JSON API	Changes made: A *Static Scan* skip option is added in the *Scan Input* > *File On-Demand* page.
Accept possible passwords from FortiMail to decompress archive file	FortiMail can send over possible passwords to decompress archive file.
Support LZH file	Files compressed with the LZH algorithms can be decompressed and scanned.
A dedicated FDN package for sniffer	Sniffer is more easily updated through a dedicated FDN package. Changes made: A new *Traffic Sniffer* module in *System* > *FortiGuard* page.
A new CLI command to authorize client devices automatically	User can decide to either manually or automatically authorize a new client device. Changes made: A new `device-authorization` CLI command.
Sniffer can extract files transmitted through raw TCP protocol	Changes made: A new *OTHER* service type in *Scan Input* > *Sniffer* page.
Allow user to turn on/off pre-filtering of certain file types	If a file type is associated with a guest VM image, it will be scanned by it. User can turn on pre-filtering so files that are non-suspicious will not be scanned by it. Changes made: New CLI command `sandboxing-prefilter`.
A newly designed job detail page	Changes made: Job detail page.
Allow user to reset scan profile settings to default	Guest images' clone number and file type association can be reset to default values. Changes made: New CLI command `reset-scan-profile`.

New Feature	Description
New CLI command to add/delete entries to check-sum White List and Black List	Changes Made: A new JSON API `/scan/policy/black-white-list`. A new *Delete* option in the *Action*: drop down menu in the *Scan Policy* > *White List* or *Scan Policy* > *Black List* pages.
Group guest VM images from different sources	Guest VM images are grouped to 3 groups: Default VMs, Customized VMs and Optional VMs. Changes Made: *Virtual Machine* > *VM Images* .
Allow user to turn on/off Sandboxing result cache	User can turn on/off the Sandboxing result cache. When it is not applied, the same file will be scanned by repeat Sandboxing. Changes made: New CLI command `sandboxing-cache`.
Activate and initialize a VM image again	Sometimes it is necessary to rebuild a VM image when it is broken. Changes made: New CLI command `vm-reset`.
Direct way to show FortiSandbox generated Malware and URL Packages	Changes made: New *Scan Input* > *Malware Package* and *Scan Input* > *URL Package* pages. The Malware Package and URL Package buttons have been removed from the *Scan Input* > *Device* page.

Upgrade Information

Upgrading from FortiSandbox 1.4.0 or later

FortiSandbox version 2.2.1 supports upgrading from version 1.4.0 or later.

Upgrading from FortiSandbox 1.3.0

FortiSandbox version 2.2.1 does not support upgrading from version 1.3.0.

Upgrading from FortiSandbox 1.2.3

FortiSandbox version 2.2.1 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<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
   Users can also try or 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 (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 2.2.1 support

The following table lists FortiSandbox version 2.2.1 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 • 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 version 5.5 and later

Resolved Issues

The following issues have been fixed in version 2.2.1. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
370892	Create a recovery page when web server crashes.
357431	User can uncheck all ports in the Sniffer Configuration page.
363626	In the UI, the IPv6 IP value is 0.0.0.0.
364766	Files with unreadable ASCII characters in its name are not scanned.
370597	Data in Executive Summary and Threat Activity reports are not accurate when a custom time period has been defined.
368103	WIN10X86 VM does not activate on a FSA_VM unit.
365680	SSH timeout does not reflect the configured *Idle Timeout* value in the UI.
365679	VM status page does not work properly if the file name contains bad characters.
366570	VM image cannot be deleted from the UI.
367038	*Threats by Hosts* page displays the wrong result when filtering the host value as *Sniffer*.
364542	File names in the Log Detail page are truncated.
357296	LDAP login does not work after reboot.

Known Issues

The following issues have been identified in version 2.2.1. 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.

FORTINET®

High Performance Network Security