FORTINET
High Performance Network Security

FortiSandbox - Release Notes

VERSION 2.2.2

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

July 28, 2016

FortiSandbox 2.2.2 Release Notes

34-222-381180-20160728

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-07-28	Initial release.

Introduction

This document provides the following information for FortiSandbox version 2.2.2 build 0155:

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

Supported models

FortiSandbox version 2.2.2 supports the FSA-1000D, FSA-3000D, FSA-3500D, and FSA-VM models.

What's new in FortiSandbox 2.2.2

The following is a list of new features and enhancements in version 2.2.2:

New Feature	Description
.dll file type scan support	Changes made: **a.** In the *Scan Policy* > *Scan Profile* page, .dll file type is added to Executables/DLL/VBS/BAT/PS1/JAR/MSI files group. If the `.dll` file type is associated with a guest VM image, it will be scanned inside it. **b.** CLI command `sandboxing-prefilter` is changed to support .dll file type pre-filtering. If enabled, .dll files which can execute inside a VM will be put to the job queue.
URL pre-filtering support	Devices like FortiMail can send all URLs inside email body to FortiSandbox. By default, all of them will be scanned inside a guest VM image. Users can turn on the URL pre-filtering to filter out non-suspicious URLs to improve system scan performance. Changes made: CLI command `sandboxing-prefilter` is changed to support URL pre-filtering. If enabled, only URLs whose web filtering rating is *Unrated* will be put to the job queue.

New Feature	Description
Allow user to configure cluster level fail-over IP for Master unit	User can configure a cluster level fail-over IP, which will be set on the new Master node after the fail-over occurs. Local IP of the previous Master node and Primary Slave node will be kept after fail-over. Changes made: CLI command `hc-settings` is changed to set cluster level fail-over IP for Master unit.

Upgrade Information

Upgrading from FortiSandbox 1.4.0 or later

FortiSandbox version 2.2.2 supports upgrading from version 1.4.0 or later.

Upgrading from FortiSandbox 1.3.0

FortiSandbox version 2.2.2 does not support upgrading from version 1.3.0.

Upgrading from FortiSandbox 1.2.3

FortiSandbox version 2.2.2 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<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 Guest 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 Microsoft Windows VM package installed, they can be installed manually or downloaded and installed through *Virtual Machine* > *VM Images* page.

By default, FortiSandbox supports a base package of 4 Windows VM images.

To manually download and install 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

   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 through port3.
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.
7. If the unit is a Master node in a cluster, configure the cluster level fail-over IP set on it.

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 2.2.2 support

The following table lists FortiSandbox version 2.2.2 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 • 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 2.2.2. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
378488	URLs submitted through JSON API are not processed correctly.
370276	Increase the number of signatures in the Malware Package.
378281	Files of Malicious rating should be added to the Malware Package.
369518	The size of manually uploaded file should be over 200MB.
373830	File type information is missing in Job Detail page for Malicious files.
377646	Failed to submit customized rescan in a Cluster environment.
376905	*File Detection* > *Summary Report*, when clicking the link at the Top Targeted Hosts widget, the page crashes.
376497	Add a *View More* button in the Job Detail page to view more job detail information.
376305	Purge pending job queue does not work as expected.
375511	Device information can be lost after upgrade.
375343	Multiple jobs might be created for a single submitted URL.
364519	Should avoid scanning multiple files at the same time if they are the same file.
357164	The format of the printed Job Detail page should follow the weekly PDF report.

Known Issues

There are no known issues that have been identified in version 2.2.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FORTINET®

High Performance Network Security