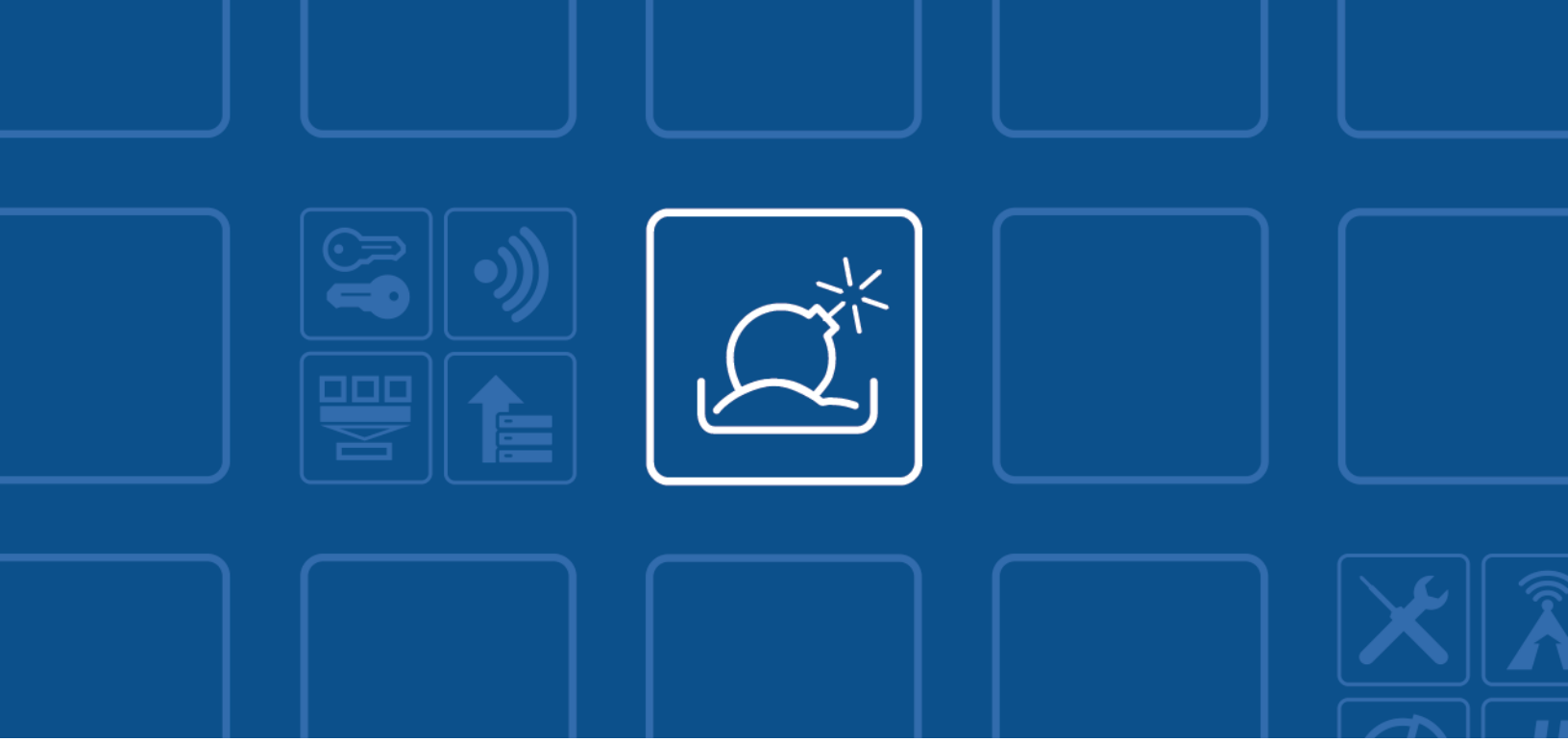
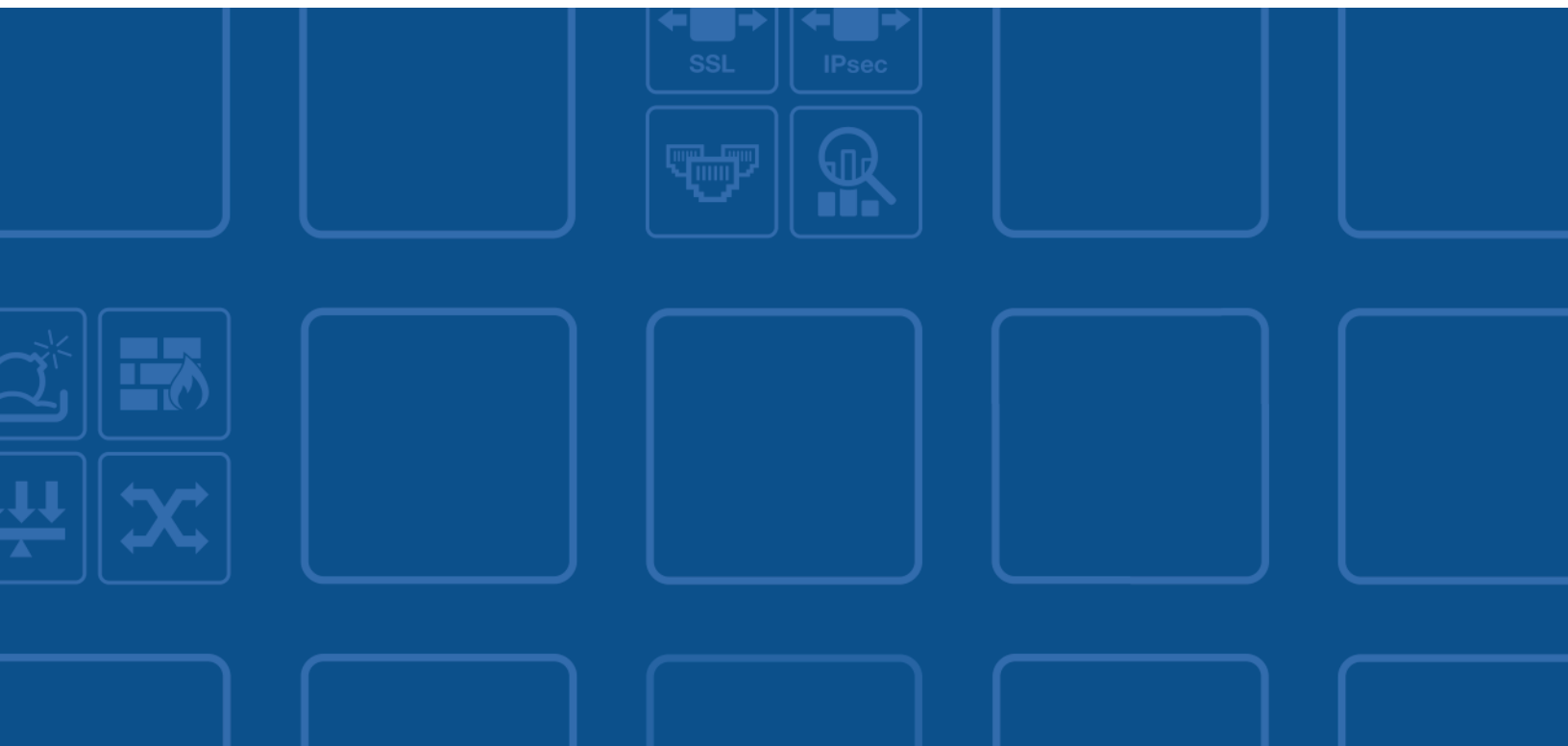


FORTINET
High Performance Network Security

FortiSandbox - Release Notes

VERSION 2.2.0



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

March 15, 2016

FortiSandbox 2.2.0 Release Notes

34-220-357555-20160315

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-03-15	Initial release.

Introduction

This document provides the following information for FortiSandbox version 2.2.0 build 0143:

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

Supported models

FortiSandbox version 2.2.0 supports the FSA-1000D, FSA-3000D and FSA-VM models.

What's new in FortiSandbox 2.2.0

The following is a list of new features and enhancements in version 2.2.0:

New Feature	Description
New GUI	The flat-style GUI and re-organized menus in a more meaningful way. Changes made: **a.** Existing menus are re-arranged **b.** Added Network menu for network management **c.** Added Virtual Machine menu for installed guest VM management **d.** Added Scan Policy menu for scan related configuration **e.** Added Scan Input menu to manage different input sources **f.** Added System Events, VM Events, Job Events, HA-Cluster Events and Notification Events sub menus under the Log & Report menu.
Modified scan profile configuration	Allow users to associate guest VMs with pre-defined file types and user defined file types. URL Scan Profile and File-based Scan Profile page are combined to one single page. Changes made: *Scan Policy > Scan Profile*

New Feature	Description
Support new guest VMs	User can purchase, install and activate the following guest VM: • Win 8.1 x86/x86_64 images • Win 10 x86/x86_64 images • Android image Changes made: *Virtual Machine* > *VM Images for VM management* *Scan Policy* > *Scan Profile* to configure file types that new guest VM can scan *System*> *FortiGuard* for FDN engine update for Android VM
Isolate VM image traffic from system traffic	User configures routing and DNS settings for guest VM and system separately. **a.** Port3 is reserved for guest VM image traffic. User can not setup a system routing entry for port3 **b.** User defines next hop and DNS for guest VM traffic **c.** User can add proxy support for VM traffic **d.** All settings in *Network* > *System Routing*, Network > System DNS are for non-VM traffic Changes made: *Dashboard* > *System Information* widget to show VM network connection status *Network* > *System Routing* to configure system static routings *Scan Policy* > *General* to configure guest VM network settings
Allow user to configure proxy for different FDN services	User can setup proxy servers for FDN update, web filtering query and Community Cloud query. Changes made: *System* > *FortiGuard*
Redesign FSA logs	Logs are grouped to different categories and made easier to search. Log servers can receive logs of all levels. Changes made: *Log & Report*
Show the time line chart of host's threat event	A bubble chart to show a time-line of threat events for a victim host. Changes made: *FortiView* > *Threats by Hosts* first and second level to show the chart.

New Feature	Description
Add port monitoring for fail-over in a Cluster	User can set up a Ping server to make sure the connection between client devices and FSA is always up. If not, a fail-over will occur after a configured period passes. Changes made: *HA-Cluster* > *Health Check*
Group pending files to different job queues. Allow user to purge job queues.	Pending jobs are grouped to different queues according to their input source and file types. User can check status and purge these queues. Changes made: CLI command: `pending-jobs` to replace previous `pending-jobs-purge`
Integrate with Bit9 end point software	User can add an adapter for the Bit9 server to receive files for scan and send their verdict back. Changes made: *File-based Detection* > *Adapter* . CLI command: `diagnose-debug adapter` to troubleshoot traffic between FSA and the Bit9 server.
Allow user to configure 'good' URL category	User can set certain URL categories to be treated as benign. Changes made: *Scan Policy* > *URL Category*
Generate malware packages in md5/sha1/sha256 format for 3rd-party to download	Changes made: *Scan Input* > *Device* > *Malware Packages*
By default the unit only keeps 3 days Clean job data	Changes made: In the *Scan Policy* > *General* page, the value of *Delete all traces of jobs of Clean or Other rating after* will be set to 3 days if it was not previously set.
By default, Medium Risk jobs are not included in malware package	Changes made: In the *Scan Policy* > *Malware Package* page, *Medium Risk* will not be checked by default.
Allow user to overwrite cloud query port	User can use a different UDP port 8888 for the Community Cloud query if UDP port 53 is blocked locally. Changes made: *System* > *FortiGuard*

New Feature	Description
Show network behavior of files in job detail page	The outgoing traffic during file scan will be added to job detail page and report. Changes made: Job detail page PDF reports

Upgrade Information

Upgrading from FortiSandbox 1.4.0 or later

FortiSandbox version 2.2.0 supports upgrading from version 1.4.0 or later.

Upgrading from FortiSandbox 1.3.0

FortiSandbox version 2.2.0 does not support upgrading from version 1.3.0.

Upgrading from FortiSandbox 1.2.3

FortiSandbox version 2.2.0 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. 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, 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 2.2.0 support

The following table lists FortiSandbox version 2.2.0 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 2.2.0. For inquires about a particular bug, please contact Customer Service & Support.

Resolved issues

Bug ID	Description
296643	Some network behaviors are not displayed in the *Chronology Chart* and *Behavior In Sequence* section of the Job Detail page.
307701	FortiSandbox multiple vulnerabilities.
308822	Special characters in file name can crash web page.
304359	*Scanning Statistics* > *Scanning Activity* widget can show wrong data.
304337	Static route entry will not be added properly when IP segments' 3octate and 4octate are `0`.
304183	*Send Test Email* does not work for email addresses under the *verdict notification to device* option.
308462	ARP cache on Firewall should be refreshed when Cluster fail-over occurs.
309928	Pending and Processing numbers are `0` sometimes.
357012	By default, keep clone number of WinXPVM1 as `0`.
355201	File name appears as *N/A* in the VM Status page.

Known Issues

The following issues have been identified in version 2.2.0. 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