FortiSandbox - Release Notes

Version 3.0.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 6, 2019
FortiSandbox 3.0.2 Release Notes
34-302-519578-20190606

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-11-01	Initial release of 3.0.2.
2019-06-06	Added 515410 and 508232 to *Resolved Issues*.

Introduction

This document provides the following information for FortiSandbox version 3.0.2 build 0041:

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.0.2 Administration Guide*.

Supported models

FortiSandbox version 3.0.2 supports the FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3500D, FSA-3000E, and FSA-VM (VMware ESXi and KVM) models.

For VM models, the total number of local VMs (default VMs + Android VMs + customized VMs) cannot exceed the local Windows key count.

What's New in FortiSandbox 3.0.2

Following is a list of new features in version 3.0.2:

- FortiSandbox VM in cluster mode supports Windows cloud VM.
- Event logs include information about important services and interface status changes.
- Support for DFS (Distributed File System) shares.

Following is a list of enhancements in version 3.0.2:

- Show customized guest VM checksum on GUI.
- Add only executables and document file types in URL package.
- Show redirected target URL in *Job Detail* page and alert emails.
- Include *Session ID* and *Sender Email ID* for FortiMail submissions.
- PDF report for archive files includes information about child files.
- Add a test to download the EICAR test file in *test-network*.

Special Notices

Licenses needed on FortiSandbox F series for customized VMs

Licenses needed to allow customized VMs on FortiSandbox F series models.

Guest VM limitation on VM models

FortiSandbox 3.0.0 added a new limitation in the allowed number of guest VMs, including customized VMs, that cannot exceed the number of purchased windows keys.

Upgrade Information

Before and after any firmware upgrade

Before any firmware upgrade, save a copy of your FortiSandbox configuration by going to *Dashboard* > *System Configuration* > *Backup*.

After any firmware upgrade, if you are using the web UI, clear the browser cache prior to login on the FortiSandbox unit to ensure proper display of the web UI screens.

Upgrading to 3.0.2

FortiSandbox 3.0.2 officially supports upgrading from version 3.0.0 and 3.0.1 to 3.0.2.

When upgrading to 3.0.2 from a version before 3.0.0, it is required that you upgrade to at least 3.0.0 first, then to 3.0.2.

Upgrading cluster environments

In a cluster environment, it is recommended to upgrade the cluster in the following order:

1. Slave devices
2. Primary Slave
3. Master

Upgrade a unit after the previous one fully boots up. After upgrade, it is highly recommended to setup a cluster level fail-over IP set, so the fail-over between Master and Primary Slave can occur smoothly.

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 does not have a 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-BASE models:**
   Download the package from ftp://fsavm.fortinet.net/images/v3.00/general_base.pkg
   FSA-2000E model:
   Download the package from ftp://fsavm.fortinet.net/images/v3.00/2000E_base.pkg
   FSA-VM00:
   Download the package from ftp://fsavm.fortinet.net/images/v3.00/VM00_base.pkg
   FSA-VMI:
   Download the package from ftp://fsavm.fortinet.net/images/v3.00/VMI_base.pkg
   Users can also purchase, download and install extra Android image packages. These packages can be downloaded from:
   Android:
   Download the package from ftp://fsavm.fortinet.net/images/v3.00/AndroidVM.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<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 and Kernel Virtual Machine (KVM) virtualization environments.

For more information, see the VM Installation Guide in 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 Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiSandbox 3.0.2 support

The following table lists FortiSandbox version 3.0.2 product integration and support information.

Web Browsers	• Microsoft Edge version 42 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 61 • Google Chrome version 59 • Opera version 54 Other web browsers may function correctly, but are not supported by Fortinet.
FortiAnalyzer	• 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.8 and later
FortiADC	• 5.0.1 and later
FortiClient	• 6.0.1 and later • 5.6.0 and later
FortiMail	• 6.0.0 and later • 5.4.0 and later • 5.3.0 and later • 5.2.0 and later
FortiManager	• 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.8 and later
FortiOS/FortiOS Carrier	• 6.0.0 and later • 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.4 and later
FortiWeb	• 6.0.0 • 5.9.0 • 5.8.0 and later • 5.7.0 and later • 5.6.0 and later

Virtualization Environment	• VMware ESXi 5.1, 5.5, or 6.0 and later • KVM

Resolved Issues

The following issues have been fixed in version 3.0.2. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
446786	Downloaded original file does not have extension.
470595	Some syslog messages do not have time stamps.
474251	VMs running in parallel caused bad condition after some time passed.
486336	Password-protected .doc file detected as clean without interaction.
494453	YARA name should not be N/A in job details.
504140	Even when verdict is ready, it is not returned to FortiMail.
504440	Should include *Detection OS* in job detail reports.
504557	Scan process stopped due to damaged file stuck in pre-scan.
504868	No ICAP response when concurrent ICAP connections are more than 10.
505524	No *submit user* in job detail PDF report for malicious URLs.
505601	Failed to replace/delete/append URL black/white list text file.
505785	Remove port3 from health check monitoring interface list.
508232	Reboot should not reset the systool package.
508232	Reboot should not reset `systool`. See also 515410.
508478	Build-in `reports.db` does not contain report table.
508569	Some URL category ratings do not match as per administration guide.
509133	Office license on custom VMs does not get activated after upgrading to 3.0.1.
509137	URL matched in white list may not be caught.
510055	User-defined black list domain should not submit to cloud.
511512	*Cannot load data now, please try again later* error in Report Center.
513387	FortiSandbox not allowing special characters in password for LDAP authentication.
514511	Netshare scan hangs when there are a large number of files.
515410	FSA-3000E clean xls and xlsx files were rated as High Risk on WIN10X64VMO16 VM. See also 508232.
516096	GUI cannot handle large white / black lists.
516106	Number of black / white list entries domain/URL/URL REGEX is limited to 1000.

Bug ID	Description
516204	High memory usage on FSA-VM00 - different values reported by SNMP, CLI output, and FortiSandbox GUI.

Known Issues

There following are the known issues that have been identified in version 3.0.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
503670	No unit took master role after HA communication failure.
511546	Interface speed query SNMP not following standard.
516032	Unable to activate Windows VM due to `VMINIT: WIN7X86SP1O16 Failed to check disk`.
518460	Primary slave won't give up the master role.
519614	Threat Activity Report does not generate if too many files are included.
521076	FortiSandbox resets network alert signature after rebooting.
521081	Admin profiles cannot be deleted if profile name has a space.