



FortiSandbox - Release Notes

Version 3.0.0

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



August 07, 2018

FortiSandbox 3.0.0 Release Notes

34-300-502976-20180807

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported models	5
What's new in FortiSandbox 3.0.0	5
Upgrade Information	7
Before and after any firmware upgrade	7
Upgrading to 3.0.0	7
Upgrading Cluster Environments	7
Upgrade procedure	7
Step 1: Upgrade the firmware	8
Step 2: Install Microsoft Windows VM package	8
Step 3: Install the Microsoft Office license file	9
Step 4: Install Windows 8.1 or Windows 10 license files	9
Step 5: Check system settings	9
Downgrading to previous firmware versions	10
FortiSandbox VM firmware	10
Firmware image checksums	10
Product Integration and Support	11
FortiSandbox 3.0.0 support	11
Resolved Issues	13
Known Issues	14

Change Log

Date	Change Description
2018-07-31	Initial release.
2018-08-02	Note added for total local VM restrictions to Supported Models section.
2018-08-07	Bug 506216 added to known issues.

Introduction

This document provides the following information for FortiSandbox version 3.0.0 build 0026:

- [Supported models](#)
- [What's new in FortiSandbox 3.0.0](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.0.0 Administration Guide*.

Supported models

FortiSandbox version 3.0.0 supports the FSA-1000D, 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 3.0.0

The following is a list of new features in version 3.0.0:

- Encrypt internal communication among HC members
- Admin user two-factor authentication
- URL Black/White list in regular expression format
- Scheduled configuration remote backup
- File submission limitation for FortiClient EMS
- .iso and .iqy file type support in Scan Profile
- Extract and scan URLs with .eml type
- BCC adapter file and URL input
- Centralized Report Centre to list all generated reports
- Centralized management of scan profile and packages
- Provide original file download link on Dashboard to support FortiGate CDR feature
- FortiADC support
- Windows Cloud VM in standalone mode
- Jumbo frame support on interfaces

The following is a list of enhancements in version 3.0.0:

- GUI menu compact mode
- Log severity level setting for local logs
- Configuration backup and restore in HC mode
- Option to disable embedded URL extraction static scan
- Support for new URL category *Newly Registered Domain* .
- Show original job info for AV rescan jobs
- Port3 duplex/speed setting
- Display Android engine version when the sample is scanned by Android VM
- New job detail page with more details
- Faster clone initialization control system
- Allow admin port other than port1
- Allow user to query job's rating with MD5 through JSON RPC

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 3.0.0

FortiSandbox 3.0.0 officially supports upgrading from version 2.4.1 and 2.5.2 to 3.0.0.

When upgrading from version 2.3.0 and 2.3.2, it is required to upgrade to 2.3.3 first, then to 2.4.1 > 3.0.0.

When upgrading from version 2.2.1 and below, the required upgrade path is: 2.2.2 > 2.3.0 > 2.3.3 > 2.4.1 > 3.0.0.

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.



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 Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiSandbox 3.0.0 support

The following table lists FortiSandbox version 3.0.0 product integration and support information.

Web Browsers	<ul style="list-style-type: none">• Microsoft Edge version 42• Microsoft Internet Explorer version 11• Mozilla Firefox version 61• Google Chrome version 59• Opera version 54 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiAnalyzer	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 5.0.1 and later
FortiClient	<ul style="list-style-type: none">• 6.0.1• 5.6.0 and later
FortiMail	<ul style="list-style-type: none">• 6.0.0• 5.4.0 and later• 5.3.0 and later• 5.2.0 and later
FortiManager	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 3.0.0. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
459436	ICAP adapter stops responding and displays error.
467048	Scan will be rejected suddenly with <code>Rejecting duplicate file from device xxx</code> message.
467320	Sandbox does not process the files from FortiGate Low-Encryption (LENC) appliances.
467539	Black/White lists tab is broken after uploading <code>.doc</code> file.
470179	<code>oftpd</code> has high CPU.
473167	Module version of GUI and FortiSandbox software version of SNMP query are different.
479595	Can't create admin account with <code>" "</code> Even for LDAP admin.
500168	FortiSandbox is scanning XML files from archive files, even if XML files have been excluded in Scan Profile.

Known Issues

The following are the known issues that have been identified in version 3.0.0. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
501012	Sandbox sent untrusted URL score 156 to FE even if the same URL was rated several minutes before.
502166	"Clean" rating results should not be sent to Syslog server when not enabled.
502353	Search results may not be correct for EMS + other criteria.
504738	"Submission Limitation" setting may not appear on GUI if only one file submitted from a FortiMail domain.
505601	Replace/Delete/Append URL black/white list text file may fail. Workaround: add or delete URLs one by one from the right panel.
506216	Internal Server Error (500 Error) after upgrade on HC members' GUI. Workaround: execute the <code>reset-widgets</code> command in the CLI after the issue happens.



FORTINET®



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.