



FortiSandbox v1.3.0 Release Notes



FortiSandbox v1.3.0 Release Notes

June 13, 2014

34-130-243557-20140613

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Fortinet Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log	4
Introduction	5
Supported models	5
What's new in FortiSandbox v1.3.....	5
Upgrade Information	6
Upgrading from FortiSandbox v1.2.3	6
Update the FortiSandbox firmware	6
Product Integration and Support	8
Web browser support	8
FortiOS support	8
FortiOS Carrier support	8
FortiMail support.....	8
FortiManager support	8
Resolved Issues	9
Known Issues	10
Known Issues.....	10
Firmware Image Checksums	11

Change Log

Date	Change Description
2014-06-09	Initial release.
2014-06-13	Updated FortiManager support information.

Introduction

This document provides a summary of enhancements, support information, installation instructions, integration, resolved and known issues in FortiSandbox v1.3.0 build 0086. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiSandbox device, see the [FortiSandbox v1.0 MR2 Administration Guide](#).

Supported models

The following models are supported on FortiSandbox v1.3.0: FSA-1000D and FSA-3000D.

What's new in FortiSandbox v1.3

The following is a list of new features and enhancements in FortiSandbox v1.3.

- Rescan malicious files
You can rescan malicious file and select to skip AV Scan, Cloud Query, or Sandboxing.
- SNMP v1, v2c, v3 support
- LDAP authentication support for administrator login
- Syslog support
Forward FortiSandbox logs to a syslog server.
- Drill down pages to view threats grouped by users, files, or devices
- Sniff multiple interfaces
Select to sniff traffic on multiple interfaces.
- Receive user details from the FortiGate
- Widget top count setting
Select the number of top entries to display in certain widgets.
- Clean file removal
Configure a specific time period to remove original files with a clean rating.

See the [Fortinet Document Library](#) for additional FortiSandbox documentation.

Upgrade Information

Upgrading from FortiSandbox v1.2.3

FortiSandbox v1.3.0 build 0086 officially supports upgrade from FortiSandbox v1.2.3.

Update the FortiSandbox firmware

Before any firmware update complete the following:

- Download the FortiSandbox firmware image and Release Notes document from the [Fortinet Customer Service & Support](#) portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Backup your configuration file. It is recommended that you create a system backup file and save this configuration to your management computer.
- Plan a maintenance window to complete the firmware update. If possible, you may want to set up a test environment to ensure that the update does not negatively impact your network.
- Once the update is complete, test your FortiSandbox device to ensure that the update was successful.



Firmware best practice: Stay current on patch releases for your current major release. Only update to a new major release or version when you are looking for specific functionality in the new major release or version.

To backup the FortiSandbox configuration:

1. In the Web-based Manager, go to *System > Dashboard > Status*.
2. In the *System Information* widget, select [*Backup/Restore*], from the *System Configuration* field.

The *System Recovery* page opens.

Figure 1: System recovery page

The screenshot shows the 'System Recovery' interface. It is divided into two main sections: 'Backup' and 'Restore'. The 'Backup' section includes a message: 'You can backup your current system configuration and restore it at a later time.' followed by a blue hyperlink 'Click here to save your backup file.' with a mouse cursor hovering over it. The 'Restore' section features a 'Restore file:' label, a 'Browse...' button, and the text 'No file selected.'. At the bottom of the interface, there are two buttons: 'Restore' and 'Cancel'.

3. Click *Click here* to save your backup file to your management computer.

To update the FortiSandbox firmware:

1. Download the FortiSandbox firmware image to server that supports file copy with the SCP command. The FortiSandbox must be able to access the SCP server.
2. In the command line interface, enter the following command string to download the firmware image from this host.

```
fw-upgrade -b -s<scp server ip> -u<user name> - p<password>  
-f<filename>
```

Product Integration and Support

Web browser support

FortiSandbox v1.3.0 supports the following web browsers:

- Microsoft Internet Explorer versions 10 and 11
- Mozilla Firefox version 29
- Google Chrome version 35

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiSandbox v1.3.0 supports the following FortiOS versions:

- v5.0.4 or later
- v5.2.0 or later

FortiOS Carrier support

FortiSandbox v1.3.0 supports the following FortiOS Carrier versions:

- v5.0.4 or later
- v5.2.0 or later

FortiMail support

FortiSandbox v1.3.0 supports the following FortiMail version:

- v5.1 or later

FortiManager support

FortiSandbox v1.3.0 is supported by the following FortiManager versions:

- v5.0.7 or later

Resolved Issues

There are no resolved issues corrected with FortiSandbox v1.3.0 build 0086. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Known Issues

The known issues table listed below does not list every bug that has been identified with FortiSandbox v1.3.0 build 0086. The bug IDs are from Fortinet's internal bug tracking system. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Known Issues

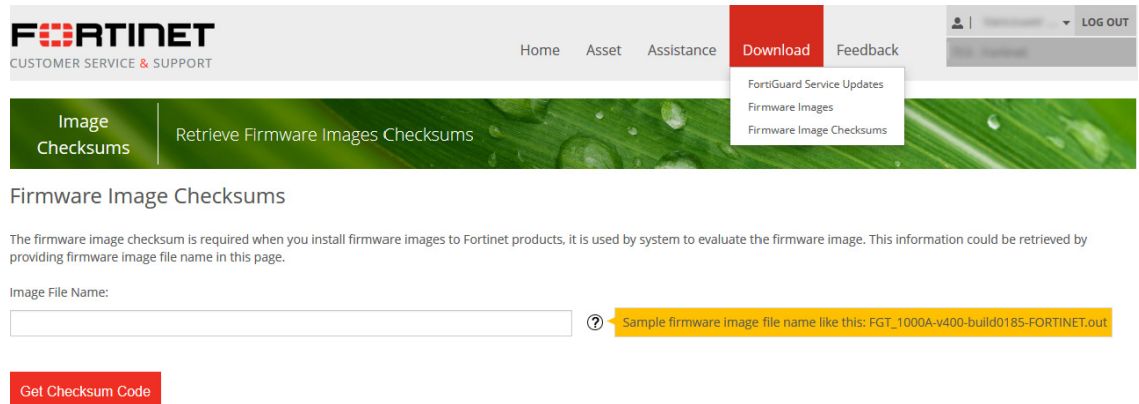
Table 1: Known issues

Bug ID	Description
0228766	In the On-Demand page, the sub-file count number for a job is not accurate.
0230769	Files with a duplicate name will be skipped during an AV rescan.
0242849	SNMP does not support IPv6 addresses.
0243098	When IPv6 traffic files are submitted from a FortiGate, the source and destination IP fields are empty.
0244491	Abnormal behavior when restoring a configuration file that the administrator does not have read/write privilege.

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*.

Figure 2: Firmware image checksum tool



The screenshot shows the Fortinet Customer Service & Support portal. The top navigation bar includes the Fortinet logo, "CUSTOMER SERVICE & SUPPORT", and links for Home, Asset, Assistance, Download, and Feedback. A user profile dropdown menu is visible with "LOG OUT" and "My Account" options. The "Download" menu is open, showing "FortiGuard Service Updates", "Firmware Images", and "Firmware Image Checksums". The "Firmware Image Checksums" page is displayed, featuring a green banner with the text "Image Checksums" and "Retrieve Firmware Images Checksums". Below the banner, there is a heading "Firmware Image Checksums" and a paragraph explaining that the checksum is required for installation and is used by the system to evaluate the firmware image. A form labeled "Image File Name:" contains an empty text input field. To the right of the input field is a help icon and a yellow tooltip that reads "Sample firmware image file name like this: FGT_1000A-v400-build0185-FORTINET.out". Below the input field is a red button labeled "Get Checksum Code".

