FortiSandbox - Release Notes

Version 3.2.0

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

October 16, 2020
FortiSandbox 3.2.0 Release Notes
34-320-610766-20201016

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-04-30	Initial release.
2020-05-06	Added 626414 to Known Issues.
2020-05-11	Added 633292 to Known Issues.
2020-08-10	Deleted duplicate entry in Known Issues.
2020-09-28	Updated What's New in FortiSandbox 3.2.0 on page 5 that two-factor authentication is not available for FortiSandbox VM.
2020-10-16	Updated Upgrading to 3.2.0 on page 7.

Introduction

This document provides the following information for FortiSandbox version 3.2.0 build 0205.

- Supported models
- What's New in FortiSandbox 3.2.0
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiSandbox device, see the *FortiSandbox 3.2.0 Administration Guide* and *FortiSandbox 3.2.0 VM Install Guide*.

Supported models

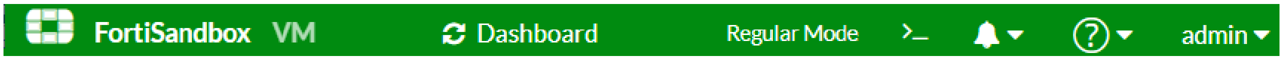
FortiSandbox version 3.2.0 supports the FSA-500F, FSA-1000D, FSA-1000F, FSA-1000F-DC, FSA-2000E, FSA-3000D, FSA-3500D, FSA-3000E, and FSA-VM (AWS, Azure, VMware ESXi, KVM, and Hyper-V) models.

What's New in FortiSandbox 3.2.0

The following is a list of new features and improvements in version 3.2.0:

- This version supports MTA on all FortiSandbox models. The MTA adapter helps with analyzing email contents, URLs, and attachments. The MTA adapter is available with a contract.
- You can choose regional DC for Windows Cloud VM.
- This version starts phasing out support for Windows XP including custom Windows XP. If you currently use Windows XP, plan to migrate to a later Windows version.
- You can set up two-factor authentication for FortiToken Cloud. This feature is only available for FortiSandbox appliances, not for FortiSandbox VM.
- A new `set-cfg-backup-key` CLI command lets you configure a password for configuration file backup and restore.
- PDF reports now support Russian language.
- When configuring a network share in *Scan Input > Network Share*, a new *Send notification email after each scan* option lets you email a summary report for each network share scan.
- In *Scan Input > Network Share*, a new *Clone* button lets you clone an existing network share. You only need to give it a different *Network Share Name*. You can clone a network share or quarantine.
- Interface ports support LACP.
- Users whose *Admin Profile* is not *Super Admin* can only view their own submissions. They cannot view other users' submissions.
- *Scan Input > File On-Demand* and *URL On-Demand* now have an *Enable AI* option to use AI mode for scanning files or URLs.

- *System > Administrators* has a new *Default On-Demand Submit settings* option to help you save time by setting defaults in *Scan Input > File On-Demand* and *URL On-Demand*. When you manually submit a file or URL, these settings are already configured. Each administrator can have their own default settings. Each HA node can have its own default settings.
  In this version, if you select *Force to scan inside the following VMs*, you cannot select Ubuntu, AndroidVM, or MACOSX.
- The Job Rescan page is redesigned to follow the On-Demand page.
- You can add FortiSandbox devices to FortiGate as a Security Fabric device. You can add a standalone FortiSandbox device or a FortiSandbox HA-Cluster primary (master) to FortiGate. For more information, see the FortiGate / FortiOS guides in the Fortinet Document Library.
- When you download and install VM images in *Virtual Machine > VM Images*, the installation does not require rebooting.
- This version introduces a new model FSA-1000F-DC that supports DC power supply.
- In the ICAP adapter, you can select the interface port that FortiSandbox listens to. The default is *port1*. See *Scan Input > Adapter*.
- This version has a new reliable TCP option for syslog server definition. In *Log & Report > Log Servers*, for *Type*, select *Syslog TCP*.
- This version support TLS 1.3 for HTTPS access.
- The green banner shows if FortiSandbox is running in regular mode or AI mode. After changing modes, refresh the page to see the change.

  To enable AI mode, use the CLI command `ai-mode -e`

  To disable AI mode, use the CLI command `ai-mode -d`
- When `sandboxing-embeddedurl` is enabled, if the URL is a direct download link, the file is downloaded and sent with the URL to be scanned.
- This version supports LDAP group filters.
- From this version on, the first time you log in using the CLI, you must set the admin password (6–64 characters).

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 before logging into FortiSandbox so that web UI screens display properly.

Upgrading to 3.2.0

FortiSandbox 3.2.0 officially supports upgrading directly from version 3.1.0, 3.1.1, 3.1.2, 3.1.3, and 3.1.4..

- When upgrading from version 3.0.0 to 3.0.5, it is required to upgrade to 3.0.6 first, then to 3.1.2 > 3.2.0.
- When upgrading from version 2.5.0 to 2.5.1, it is required to upgrade to 2.5.2 first, then to 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0.
- When upgrading from version 2.4.0, it is required to upgrade to 2.4.1 first, then to 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0.
- When upgrading from version 2.3.0 to 2.3.2, it is required to upgrade to 2.3.3 first, then to 2.4.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0.
- When upgrading from version 2.2.1 and earlier, the required upgrade path is 2.2.2 > 2.3.0 > 2.3.3 > 2.4.1 > 2.5.2 > 3.0.0 > 3.0.6 > 3.1.2 > 3.2.0.

After upgrading, FortiSandbox stops processing files until the latest rating engine is installed either by FDN update or manually.

Every time FortiSandbox boots up, it checks FDN for the latest rating engine.

If the rating engine is not available or out-of-date, you get these notifications:

- A warning message informs you that you must have an updated rating engine.
- The *Dashboard System Information* widget displays a red blinking *No Rating Engine* message besides *Unit Type*.

If necessary, you can manually download an engine package from Fortinet Customer Service & Support.

If the rating engine is not available or out-of-date, FortiSandbox functions in the following ways:

- FortiSandbox still accepts on-demand, network share, and RPC submissions, but all jobs are pending.
- FortiSandbox does not accept new devices or FortiClients.
- FortiSandbox does not accept new submissions from Sniffer, Device, FortiClient, or Adapter.

Upgrading cluster environments

Before upgrading, it is highly recommended that you set up a cluster IP set so the failover between primary (master) and secondary (primary slave) can occur smoothly.

In a cluster environment, use this upgrade order:

1. Upgrade the workers (regular slaves) and install the new rating engine. Then wait until the devices fully boot up.
2. Upgrade the secondary (primary slave) and install the new rating engine. Then wait until the device fully boots up.
3. Upgrade the primary (master). This causes HA failover.
4. Install the new rating engine on the old primary (master) node. This node might take over as primary (master) node.

Upgrade procedure

When upgrading from 3.1.0 or later and the new firmware is ready, you will see a blinking *New firmware available* link on the dashboard. Click the link and you will be redirected to a page where you can either choose to download and install an available firmware or manually upload a new firmware.

Upgrading FortiSandbox firmware consists of the following steps:

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> -t<ftp|scp> -f<file path>
   ```
3. When upgrading via the Web UI, 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.

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, Hyper-V, Nutanix, 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 3.2.0 support

The following table lists FortiSandbox version 3.2.0 product integration and support information.

Web Browsers	• Microsoft Edge version 80 • Mozilla Firefox version 74 • Google Chrome version 80 • Opera version 67 Other web browsers may function correctly but are not supported by Fortinet.
FortiAnalyzer	• 6.4.0 (all FortiSandbox models except FSA-1000F-DC) • 6.2.0 and later • 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	• 5.4.0 • 5.3.0 and later • 5.0.1 and later
FortiClient	• 6.2.0 and later • 6.0.1 and later • 5.6.0 and later
FortiEMS	• 6.2.0 and later • 6.0.5 and later
FortiMail	• 6.2.0 and later • 6.0.0 and later • 5.4.0 and later • 5.3.0 and later • 5.2.0 and later
FortiManager	• 6.2.1 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later
FortiOS/FortiOS Carrier	• 6.2.0 and later • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later

	• 5.2.0 and later
FortiWeb	• 6.3.2 • 6.2.0 and later • 6.0.0 and later • 5.8.0 and later • 5.6.0 and later
FortiProxy	• 1.2.3
Virtualization Environment	• VMware ESXi: 5.1, 5.5, 6.0, or 6.5 and later • KVM: Linux version 4.15.0 qemu-img v2.5.0 • Microsoft Hyper-V: Windows server 2016

Resolved Issues

The following issues have been fixed in version 3.2.0. For inquiries about a particular bug, contact Customer Service & Support.

Resolved issues

Bug ID	Description
573390	LDAP wildcard administrators do not support AD groups.
578402	FortiSandbox does not exclude whitelist from malware package.
578434	FortiSandbox does not give confirmation ID in the log.
579978	Restored configuration restores unprocessed alert setting.
583569	The administrator with token authorization fails to test login.
583897	The connection fails if you use FortiManager as the web filter server.
584257	The setting from CLI command `set-tlsver` does not synchronize during the HA failover.
584772	Creating a new Bit9 adapter causes the GUI to crash.
595761	The CLI command `test-network` does not display the server addresses for FDN and community cloud.
597427	FortiClient cannot connect to FortiSandbox.
601190	The downloaded file from the embedded URL in a HTML file isn’t sent to the sandbox for scan.
602846	Job details don't display *Static File Scan(AI)* if the job is rated by static scan and AI is on.
603939	FortiSandbox Azure does not support using service principal (the Client ID).
612620	FortiSandbox Azure does not delete VM clone and relative resources after the VM is deleted from the GUI.
612621	FortiSandbox Azure creates public IP on customized VM clone.
612628	FortiSandbox Azure loses installed customized VMs if it is stopped and started from Azure portal manually.

Known Issues

The following issues have been identified in version 3.2.0. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Bug ID	Description
575345	Restored configuration did not restore memory scan YARA rules.
620331	Adapter configuration is lost after upgrading to 3.2.0.
622675	`Fortimail-expired` is be reset after upgrading to 3.2.0.
623677	Configuration restoration is allowed among different FortiSandbox models.
626414	Push authentication does not work when logging back into FortiSandbox. The FTC option is limited to manual OTP entry. 2FA using push does not currently work.
627458	FSA-3500D uses high CPU if there are eight Windows10 VM clones enabled.
633292	In an HA-Cluster, a memory leak might cause a worker (slave) process to use excessive memory.