

Best Practices and Troubleshooting Guide

FortiSandbox 4.4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



February 22, 2024

FortiSandbox 4.4.0 Best Practices and Troubleshooting Guide

34-440-976530-20240222

TABLE OF CONTENTS

Overview	5
Know your FortiSandbox	5
FortiSandbox and FortiGate process flow	5
FortiSandbox and FortiMail process flow	6
Additional information	7
Installing FortiSandbox	8
Upgrading cluster environments	8
Downgrading to previous firmware versions	8
Business continuity	9
General maintenance	10
Backing up the FortiSandbox configuration	10
Restoring the FortiSandbox configuration	10
Scheduling maintenance tasks for off-peak hours	10
Maintaining database integrity	10
Maintaining storage integrity	11
Hardening	12
Building security into FortiSandbox	12
Physical security	12
Vulnerability - monitoring PSIRT	12
Firmware	12
Encrypted protocols	13
Strong ciphers	13
FortiGuard databases	13
Penetration testing	13
Trusted Hosts	13
Limit login user's access right	13
Other recommended actions user can take	14
Advanced procedures	15
Improving scan performance	15
Understanding Inline Block feature	16
Considerations	17
Hot-swapping hard disk	18
Recovering system using Rescue Mode	19
Revalidating Windows license key	25
Resetting user's admin password	26
Resizing the data volume on AWS	27
Resizing the data disk for FortiSandbox on Azure	28
Setting up a FortiSandbox VM00 as Primary node for high availability	31
Troubleshooting guidelines	33
Troubleshooting Dashboard warnings	33
Windows VM	33

FortiGuard connectivity servers	34
VM Internet access	35
Troubleshooting system resource issues	35
Troubleshooting cloning issues	36
Troubleshooting the Job Queue	37
Troubleshooting NetShare issues	38
NFSv4 error	38
Troubleshooting detection issues	38
Trace a file	38
Known malware not detected	39
Change Log	41

Overview

This guide is a collection of best practices and troubleshooting guidelines for using FortiSandbox. Use these guidelines to get the most of your FortiSandbox products, maximize its performance, and avoid potential problems.

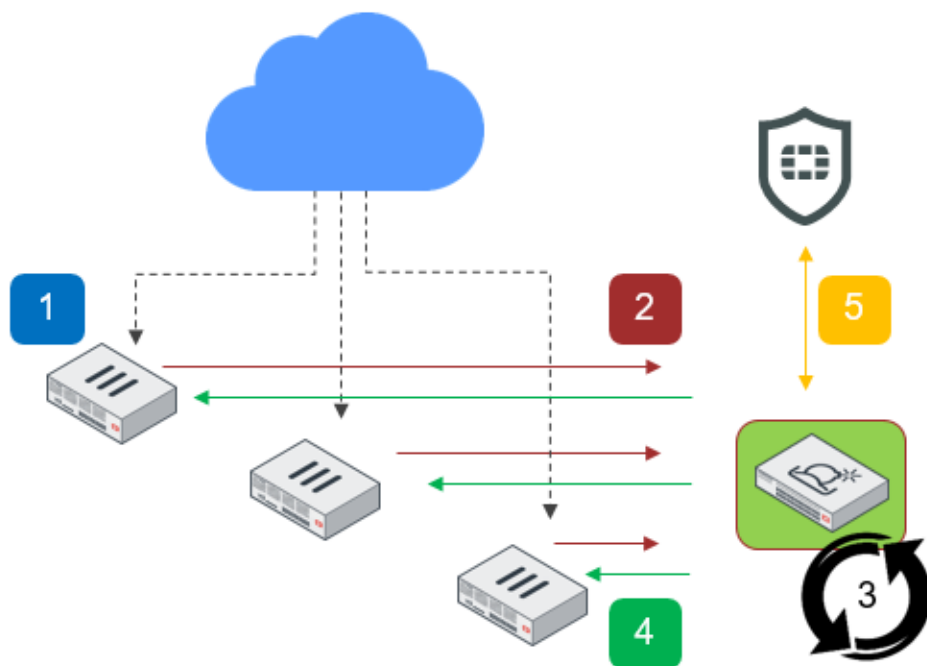
Know your FortiSandbox

Understanding the process flow of your FortiSandbox can provide additional awareness and information that may help you in troubleshooting.

For configuring FortiSandbox, see [Installing FortiSandbox on page 8](#). For troubleshooting, see [Troubleshooting guidelines on page 33](#).

FortiSandbox and FortiGate process flow

The FortiSandbox (acting as a server) receives files from FortiGate (acting as client). Then, it provides an updated Threat Intelligence database back to the client.

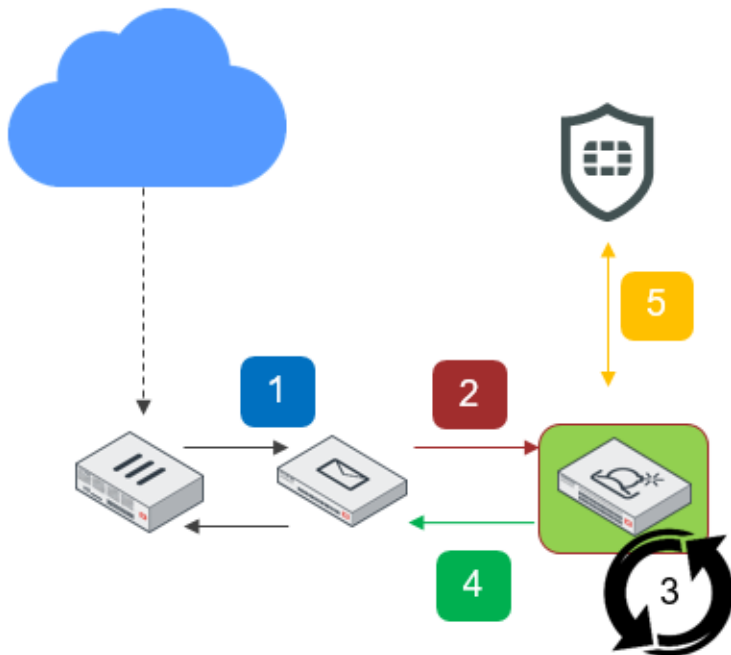


1. FortiGate extracts files from the network traffic. It uses the AntiVirus scan profile for sandboxing feature. File size limit apply. Before forwarding previously seen files, it crosschecks its cache (known as Threat Intelligence DB or Malware package).
2. FortiGate queries FortiSandbox first if previously forwarded. If not, FortiGate forwards the file along with the serial number, IP address, and VDOM information.

3. The submission goes through a series of scan flow stages. A verdict can be reached at any stage. The last stage is VM Scan which takes 2-3 mins. FortiSandbox keeps the submissions and its results for 60 days for Malware verdict and 3 days for Clean verdict.
4. FortiGate pulls the latest Threat Intelligence DB every 2 mins. The DB contains a list of malicious file checksums and related URLs. FortiGate also queries the verdict for logging.
5. FortiSandbox checks FortiGuard every hour and downloads new packages and engines. FortiSandbox can share malicious files and URL with FortiGuard when Sandbox Community is enabled. FortiSandbox can forward detection statistics to FortiGuard for analysis of trending threats when enabled in configuration.

FortiSandbox and FortiMail process flow

The FortiSandbox (acting as a server) receives files and URLs embedded in emails from FortiMail (acting as client). The client waits for the verdict before releasing any email as safe (clean).



1. FortiMail receives email from the Internet or one of the clients. It uses the AntiVirus scan profile for sandboxing feature. It checks for any file attachments and embedded URLs. On extracting URLs, the default count is 10.
2. FortiMail queries FortiSandbox first. If results are already known and up-to-date, then use the previous result. Otherwise, it forwards the files and URLs to FortiSandbox. It waits for the verdict before releasing the email.
3. Upon receipt of submission from FortiMail, a job id is created. The submission goes through a series of scan flow stages. A verdict can be reached at any stage. FortiSandbox keeps the submissions and its results for 60 days for Malware verdict and 3 days for Clean verdict.
4. FortiMail pulls the result every 10 seconds of the submission until a verdict is reached.
5. FortiSandbox checks FortiGuard every hour and downloads new packages and engines. FortiSandbox can share malicious files and URLs with FortiGuard when Sandbox Community is enabled. FortiSandbox can forward detection statistics to FortiGuard for analysis of trending threats when enabled in configuration.

Additional information

For product and feature guides, go to the Fortinet Document Library at <http://docs.fortinet.com>.

For procedures on how to implement these best practices, see the *FortiSandbox Administration Guide* in the [Fortinet Document Library](#).

For customer service and technical support, go to <https://support.fortinet.com>.

For technical notes, how-to articles, FAQs, and links to the technical forum and technical documentation, go to the Fortinet Knowledge Base at <http://kb.fortinet.com/kb>.

Installing FortiSandbox

Plan your installation carefully and select the FortiSandbox model(s) that meet your requirements.

- Plan the size of your installation appropriately. Ensure you also plan for future sandboxing requirements. Refer to the [FortiSandbox Data Sheet](#) for performance information of each model.
- Ensure you have remote serial console or virtual console access.
- Ensure that a local FTP or SCP server is available on a network local to the FortiSandbox.

Before any firmware upgrade, save a copy of your FortiSandbox configuration by going to *Dashboard > Status System Information* widget, and clicking the *Backup/Restore* icon in the *System Configuration* line.

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

Upgrading cluster environments



In a cluster environment, we recommended upgrading the cluster in the following order:

1. Worker devices
2. Secondary device
3. Primary device

Upgrade a unit after the previous one fully boots up. After upgrade, we highly recommend setting up a cluster level failover IP set for a smooth failover between primary and secondary.

Downgrading to previous firmware versions

Downgrading to previous firmware versions is not supported.

Business continuity

- Ensure the FortiSandbox has a valid subscription to the Sandbox Threat Intelligence in order to continue the download of the latest engines and databases and access the FortiGuard for File and Web Filtering Queries.
- Ensure the FortiSandbox environment has a stable and/or uninterruptible power supply. A power loss can damage FortiSandbox databases.
 - If there is unexpected power loss, revert to a known good backup of the configuration. See [Restoring the FortiSandbox configuration on page 10](#).
 - If a shut down or reboot is necessary, always perform gracefully. Removing power without a graceful shutdown can damage FortiSandbox databases. See [Maintaining database integrity on page 10](#).
- Ensure there are spare parts on site such as fans, power supplies, disks, and so on.

General maintenance

Perform general maintenance tasks such as backup and restore so that you can revert to a previous configuration if necessary.

Backing up the FortiSandbox configuration

- Perform regular backups to ensure you have a recent copy of your FortiSandbox configuration.
- If your FortiSandbox is a virtual machine, you can also use VM snapshots.

Restoring the FortiSandbox configuration

Restore configuration backups to the same FortiSandbox model with the same firmware. Do not restore a configuration backup to a FortiSandbox model with different firmware.

Scheduling maintenance tasks for off-peak hours

We recommend scheduling maintenance tasks for off-peak hours whenever possible including tasks such as:

- Firmware upgrade
- System topology change
- Swapping failed hard disk

Maintaining database integrity

To maintain database integrity, **never** power off a FortiSandbox unit without a graceful shutdown. Removing power without a proper shutdown can damage FortiSandbox databases. Always use the following shutdown command before powering off.

```
shutdown
```

We highly recommend connecting FortiSandbox units to an uninterruptible power supply (UPS) to prevent unexpected power issues that might damage internal databases.

Maintaining storage integrity

To keep FortiSandbox storage healthy, we recommend regularly checking the *Disk Usage* in the *System Resources* widget or you may setup external logging.

If disk usage is increasing rapidly and does not stabilize after a period of time, then review your policy for retaining submitted files. To do that, go to *system > Settings > Data Storage* to the *Delete all traces of jobs of Clean or Other rating* after setting and set a shorter time period.

Hardening

System hardening reduces security risk by eliminating potential attack vectors and shrinking the system's attack surface. This section covers some actions that can be used.

Building security into FortiSandbox

The FortiSandbox firmware, FortiSandbox hardware devices, and FortiSandbox virtual machines (VMs) are built with security in mind, so many security features are built into the hardware and software. Fortinet maintains an ISO:9001 certified software and hardware development processes to ensure that FortiSandbox products are developed in a secure manner.

Physical security

Install the FortiSandbox in a physically secure location. Physical access to the FortiSandbox can allow it to be bypassed, or other firmware could be loaded after a manual reboot. Optionally, disable the maintainer account with CLI command `set-maintainer`. Note that doing this will make you unable to recover administrator access using a console connection as all of the administrator credentials are lost.

Vulnerability - monitoring PSIRT

Product Security Incident Response Team (PSIRT) continually tests and gathers information about Fortinet hardware and software products, looking for vulnerabilities and weaknesses. The findings are sent to the Fortinet development teams, and serious issues are described, along with protective solutions, in advisories listed at <https://www.fortiguard.com/psirt>.

Firmware

Keep the FortiSandbox firmware up to date. The latest patch release has the most fixed bugs and vulnerabilities, and should be the most stable. Firmware is periodically updated to add new features and resolve important issues.

- Read the release notes. The known issues may include issues that affect your business.
- Do not use out of support firmware. Review the product lifecycle and plan to upgrade before the firmware expires.
- Optionally, subscribe to the Fortinet firmware RSS feed: <https://pub.kb.fortinet.com/rss/firmware.xml>.

Encrypted protocols

Use encrypted protocols whenever possible, for example, SNMPv3 instead of SNMP, SMTPS instead of SMTP, ICAP over SSL instead of ICAP, SSH instead of telnet, HTTPS instead of HTTP for Webpage visit and JSON API calls, and encrypted logging instead of TCP.

Strong ciphers

Force higher levels of encryption and strong ciphers for HTTPS access to web site and JSON API calls:

```
set-tlsver -e3
```

FortiSandbox already sets to use higher levels of encryption and strong ciphers for communications with Fortinet fabric devices.

FortiGuard databases

Ensure that FortiGuard databases and engines, such as *AntiVirus*, *Network Alerts*, *Rating* and *Tracer*, are updated punctually.

Penetration testing

Test your FortiSandbox to try to gain unauthorized access, or hire a penetration testing company to verify your work.

Trusted Hosts

Limit access to the FortiSandbox to a management interface on a management network. Trusted hosts can also be used to specify the IP addresses or subnets that can log in to the FortiSandbox. When authenticating to the FortiSandbox, implement two-factor authentication (2FA). This makes it significantly more difficult for an attacker to gain access to the FortiSandbox.

Limit login user's access right

The features that a login user can access should be limited to the scope of that user's work to reduce possible attack vectors. The admin profile tied to the user account defines the areas on the FortiSandbox that the user can access, and what they can do in those areas. The list of users with access should be audited regularly to ensure that it is current.

Other recommended actions user can take

The following general administrative settings are recommended:

- Set the idle timeout time for login users to a low value, preferably less than ten minutes.
- In Interfaces page, limit access rights for network ports.
- Replace the certificate that is offered for HTTPS access with a trusted certificate that has the FQDN or IP address of the FortiSandbox.
- Do not use shared accounts to access the FortiSandbox. Shared accounts are more likely to be compromised, are more difficult to maintain as password updates must be disseminated to all users, and make it impossible to audit access to the FortiSandbox.
- Set an encryption key for backed up configuration files with CLI command `set-cfg-backup-key`.

Advanced procedures

These topics contain advanced best practices to help you make better use of FortiSandbox.

- [Improving scan performance on page 15](#)
- [Understanding Inline Block feature on page 16](#)
- [Hot-swapping hard disk on page 18](#)
- [Recovering system using Rescue Mode on page 19](#)
- [Revalidating Windows license key on page 25](#)
- [Resetting user's admin password on page 26](#)
- [Resizing the data volume on AWS on page 27](#)
- [Resizing the data disk for FortiSandbox on Azure on page 28](#)
- [Setting up a FortiSandbox VM00 as Primary node for high availability on page 31](#)

Improving scan performance

A unit processes files at a certain rate. There are ways to improve the unit's scan power. The following suggestions help to optimize your system's scan performance.

1. Only keep jobs with a clean rating for a short period.

If you are not concerned about processed files with a clean rating, you can configure the system to remove them after a short period. This saves system resources and improves system performance.

To do that, go to *System > Settings > Data Storage* and set a short time period in the *Delete all traces of jobs of Clean or Other rating after* section.

2. Turn on FortiSandbox Pre-Filtering of certain file types.

By default, if a file type is associated with a Windows VM image, all files of this file type are scanned inside it. Sandboxing scans inside a Windows VM is a slow and intensive process. For information about throughput, see the [FortiSandbox datasheet](#) for your model.

You can enable *Scan Policy and Object > Scan Profile* on some file types. When enabled, files of that file type are inspected by an advanced FortiGuard engine and only suspicious files will be scanned inside a VM.

The *Log & Report > File statistics > Top File Types widget > Scanned by Sandboxing* gives you hints on which file types can skip sandboxing.

Use the CLI command `sandboxing-prefilter -e` to enable sandboxing.

3. Associate every file type to only one VM type.

Theoretically, one file should be scanned inside all enabled VM types to get best malware catch rate. However, to improve scan performance, every file type should be associated with only one VM type.

4. Allocate clone numbers of each VM type according to the distribution of file types.

Each unit can only prepare a limited number of guest image clones. The number is determined by installed Windows license keys. Allocate clone numbers according to the distribution of file types. For example, if there are a lot of Office files and WIN7X86VM is associated with Office files, you can decrease the clone number of other VM types and increase the clone number of the WIN7X86VM.

If there are many pending jobs, use the `pending-jobs` CLI command or go to *Scan Job > Job Queue* to check which file type has the longest queue and increase clone numbers of its associated VM type.

5. Reduce enabled Windows VM types.

Each enabled Windows VM type requires system memory runtime to store them. The more enabled types, the less system memory is available for scanning. This is especially the case when you enable customized images of a large size. To improve scan performance and clone system stability, we recommended reducing enabled VM types.

6. Do not associate VM types to archive files.

FortiSandbox checks every file inside an archive file and puts it in its own job queues according to *Scan Profile* settings. If an archive file is scanned inside a VM, the archive file is opened but the files inside the archive file are not scanned; so sandboxing scan an archive file itself is not effective in detecting malware. Therefore we recommend not associating VM types with archive files.

Understanding Inline Block feature

The Inline Block feature allows FortiGate device fabric integration to perform inline blocking on known and unknown malware. This feature was introduced in FortiSandbox 4.2.0 and FortiOS 7.2.0.

To configure Inline Block on:

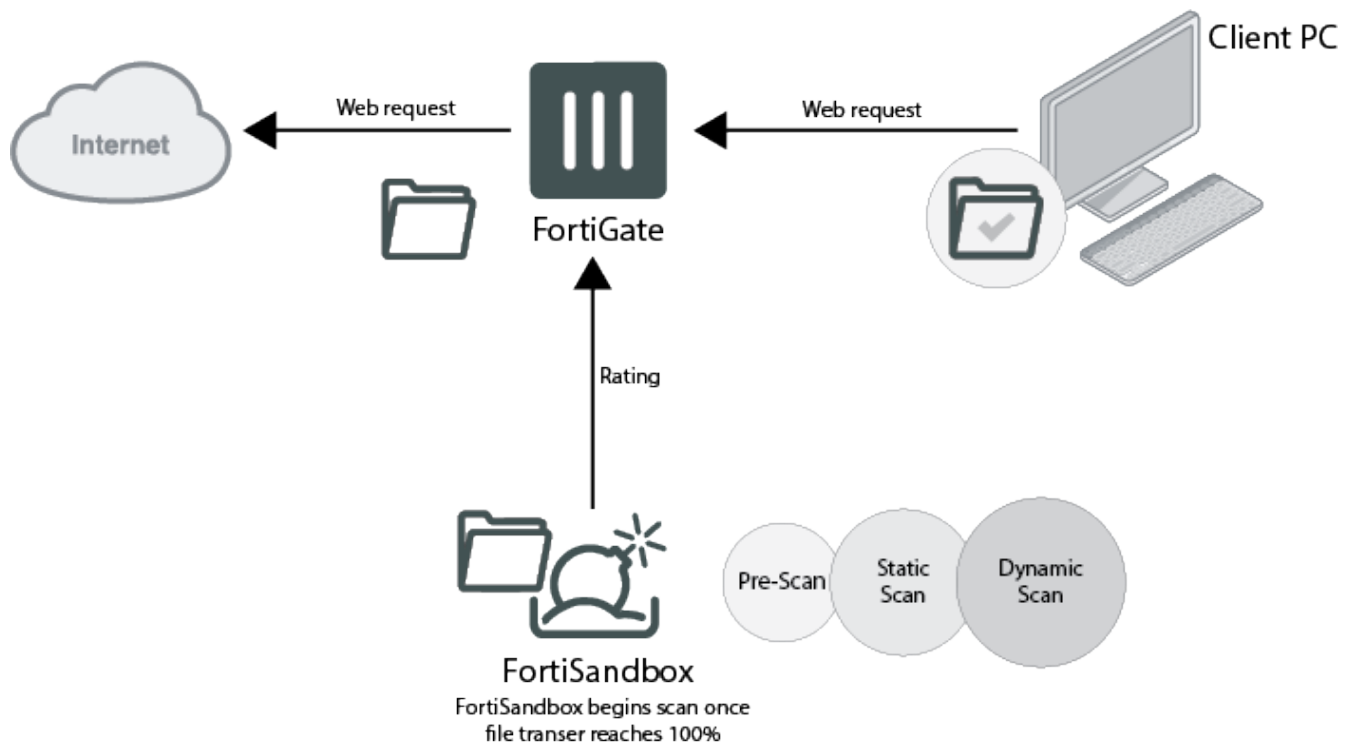
- FortiSandbox, see [Inline Block Policy](#).
- FortiGate, see [FortiSandbox inline scanning](#). Make sure that the Inspection Mode is set to `proxy`.

When Inline Block is enabled, FortiGate holds part of the file until the FortiSandbox has provided its rating. The FortiSandbox performs a series of Static Scan modules:

- Active Content check searches for any executable code, macro and scripts.
- Pre-filtering is a Scan Profile configuration.
- FortiSandbox Community Cloud check queries the FortiGuard for any submissions by other FortiSandbox devices located worldwide who contributes to the community.
- Static Scan engines are the Antivirus and AI engines using pattern matching and models.

In most cases, these scans only take a few seconds.

When the FortiSandbox determines that a Dynamic Scan is required, the turnaround time may take a minute for Office and PDF files and a few minutes for executable files.



Considerations

Office and PDF files

The FortiSandbox 2000E, 1500G and higher models allow for the lowering of the Dynamic Scan timeout. We recommend you lower timeout time to 45 seconds (or, as low as 30 seconds) to allow the FortiSandbox to provide the rating within the expected time limit of the FortiGate. That is configurable via *Scan Profile > Advanced tab*.

Executable files

FortiSandbox scans executable files thoroughly by sending the files to its Static AI and Dynamic AI Analysis stages. If FortiSandbox can provide its rating based on static AI analysis back to the FortiGate, then the file can be allowed for clean or blocked if suspicious rating. If the FortiSandbox needs to continue with the dynamic AI analysis, it sends a notification to FortiGate for continuity that it requires more time. Meanwhile, the FortiGate will take action on the file based on its configuration. The default FortiGate setting is to allow download of files on time out or scan error from FortiSandbox. The configuration can be changed to block the file with a replacement message and try downloading again at a later time. When the user tries to download again, FortiSandbox will have known the rating and should be able to response quickly.

Other considerations:

- Inline Block relies on the resources of the FortiSandbox to be able to quickly bring up the VMs for Dynamic Scan. Only the following models can meet the resource requirement: 3000F, 3000E, 2000E, and 1500G. The other deployment models can possibly meet the requirement depending on its current capacity.
- Enable sandboxing prefiltering on all file types with CLI command `sandboxing-prefilter`.

- Review the capacity of the FortiSandbox based on the *Scan Performance* [widget](#) and [dashboard](#). If the pending time is too high, monitor and evaluate if the current deployment needs additional FortiSandbox units.

Hot-swapping hard disk

If a hard disk on a FortiSandbox unit fails, it must be replaced. FortiSandbox devices support hardware RAID and the hard disk can be replaced while the FortiSandbox unit is running, also known as hot-swapping.

The following table shows the RAID level on different models and supports hot-swapping hard disk:

FortiSandbox model	RAID Level
FSA-2000E	RAID-1
FSA-3000E	RAID-10
FSA-3000F	RAID-10
FSA-1500G	RAID-1

To identify which hard disk failed the following diagnostic commands are available:

<code>hardware-info</code>	Display general hardware status information. Use this command to view CPU, memory, disk, and RAID information, and system time settings.
<code>disk-attributes</code>	Display system disk attributes.
<code>disk-errors</code>	Display any system disk errors.
<code>disk-health</code>	Display disk health information.
<code>disk-info</code>	Display disk hardware status information.
<code>raid-hwinfo</code>	Display RAID hardware status information.

To hot-swap a hard disk on a device that supports hardware RAID, simply remove the faulty hard disk and replace it.



Electrostatic discharge (ESD) can damage FortiSandbox equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiSandbox chassis.

When replacing a hard disk, you need to first verify that the new disk has the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiSandbox unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.

The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

The FortiSandbox unit will automatically add the new disk to the current RAID array. The status appears on the console. The RAID Management page will display a green checkmark icon for all disks and the *RAID Status* area will display the progress of the RAID re-synchronization/rebuild.



Once a RAID array is built, adding another disk with the same capacity will not affect the array size until you rebuild the array by restarting the FortiSandbox unit.

Recovering system using Rescue Mode

The purpose of Rescue Mode is to provide the ability to boot using some other boot method instead of the system's boot loader or hard drive when encountering a failure. Using Rescue Mode through the console port, you can restore the system using a firmware image located on an external server or USB drive.

Main menu

To access the Rescue Mode feature, first log in to the FortiSandbox from the console port and open the CLI window. Execute the CLI command `reboot` then respond yes [y] when prompted to get into Rescue Mode. The console will disconnect, then after one or two minutes, the rescue menu will display. It will continue to boot up if no options are selected within 10 seconds.

```
[Q]: Quit menu and continue to boot.
[G]: Get firmware image from TFTP server.
[W]: Get firmware image from HTTP server.
[T]: Get firmware image from FTP server.
[U]: Get firmware image from another USB drive.
[I]: System information.
[F]: Format data device.
[C]: Check device filesystem.
[H]: Display this list of options.

Enter Q,G,W,T,U,I,F,C or H:
```

The options are Q, G, W, T, U, I, F, C or H.

- Q will quit the menu and continue to boot into the FortiSandbox system.

Retrieving the firmware image from the TFTP server

Entering G from the main menu will open a sub-menu with options for retrieving and upgrading the firmware image from the TFTP server.

- Entering C from this sub-menu allows you to configure the network and image parameters

```

Enter C,R,N,T or Q:C

Available port list: port1 port3
Enter image download port number [port1]:
Enter local IP address [192.168.0.99]:10.59.2.62
Enter local subnet mask [255.255.255.0]:
Enter local gateway [192.168.0.1]:10.59.2.1
Enter DNS [208.91.112.53]:
Enter remote server IP address [192.168.0.199]:10.59.2.148
Enter firmware file name [image.out]:FSA_2000E-v300-build0060-FORTINET.out
Format boot device before install image (Y/N) [N]:y
Applying network parameters ... OK

[C]: Configure network & image parameters.
[R]: Review network & image parameters.
[N]: Diagnose networking (ping).
[T]: Initiate firmware transfer.
[Q]: Quit this menu.

```

Enter *R* to review the parameters:

```

Enter C,R,N,T or Q:r

Image download port: port1
Local IP address: 10.59.2.62
Local subnet mask: 255.255.255.0
Local gateway: 10.59.2.1
DNS: 208.91.112.53
Remote server IP address: 10.59.2.148
Firmware file: /image/image.deb.2000E
Format boot device: Y

```

Enter *N* to test the network:

```

Enter C,R,N,T or Q:N

Enter the IP address for ping or [Q/q] to quit this menu:10.59.2.148
PING 10.59.2.148 (10.59.2.148): 56 data bytes
64 bytes from 10.59.2.148: seq=0 ttl=64 time=0.401 ms
64 bytes from 10.59.2.148: seq=1 ttl=64 time=0.284 ms
64 bytes from 10.59.2.148: seq=2 ttl=64 time=0.201 ms
64 bytes from 10.59.2.148: seq=3 ttl=64 time=0.235 ms
64 bytes from 10.59.2.148: seq=4 ttl=64 time=0.319 ms

--- 10.59.2.148 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.201/0.288/0.401 ms

Enter the IP address for ping or [Q/q] to quit this menu:Q

```

Enter *T* to download the image and install a new image, and the FortiSandbox will reboot automatically:

```

[C]: Configure network & image parameters.
[R]: Review network & image parameters.
[N]: Diagnose networking (ping).
[T]: Initiate firmware transfer.
[Q]: Quit this menu.

Enter C,R,N,T or Q:T

Connect to tftp server 10.59.2.148:
98% [=====]
Image image.deb.2000E was received.

Format the boot device, then install and launch this firmware? [Y/N]:y

Verifying image sections ... OK
Formatting boot device ... OK
Installing image ... █

```

Once successfully booted up, you can log in again with your username and password:

```
Starting FortiSandbox
Check journal on boot device
Initializing core system ...
Detected SN: FSA2KE3117000007
Checking raid settings ...
Initializing hard drive devices ...
Initializing OS components ...
Initializing virtual components ...
Initializing database ...
Initializing scan components ...
Verifying the system ...
Starting system ...

FortiSandbox login: █
```

Retrieving the firmware image from the HTTP server

Entering *W* from the main menu will open a sub-menu with options for retrieving and upgrading the firmware image from the HTTP server.

- Entering *C* from this sub-menu allows you to configure the network and image parameters:

```
Enter C,R,N,T or Q:c

Available port list: port1 port3
Enter image download port number [port1]:
Enter local IP address [192.168.0.99]:10.59.2.62
Enter local subnet mask [255.255.255.0]:
Enter local gateway [192.168.0.1]:10.59.2.1
Enter DNS [208.91.112.53]:
Enter remote server IP address [192.168.0.199]:10.59.2.148
Enter firmware file name [image.out]:/image/image.deb.2000E
Format boot device before install image (Y/N) [N]:y
Applying network parameters ... OK

[C]: Configure network & image parameters.
[R]: Review network & image parameters.
[N]: Diagnose networking (ping).
[T]: Initiate firmware transfer.
[Q]: Quit this menu.
```

Enter *R* to review the parameters.

```
Enter C,R,N,T or Q:r

Image download port: port1
Local IP address: 10.59.2.62
Local subnet mask: 255.255.255.0
Local gateway: 10.59.2.1
DNS: 208.91.112.53
Remote server IP address: 10.59.2.148
Firmware file: /image/image.deb.2000E
Format boot device: Y
```

Enter *N* to test the networking.

```
Enter C,R,N,T or Q:N

Enter the IP address for ping or [Q/q] to quit this menu:10.59.2.148
PING 10.59.2.148 (10.59.2.148): 56 data bytes
64 bytes from 10.59.2.148: seq=0 ttl=64 time=0.401 ms
64 bytes from 10.59.2.148: seq=1 ttl=64 time=0.284 ms
64 bytes from 10.59.2.148: seq=2 ttl=64 time=0.201 ms
64 bytes from 10.59.2.148: seq=3 ttl=64 time=0.235 ms
64 bytes from 10.59.2.148: seq=4 ttl=64 time=0.319 ms

--- 10.59.2.148 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.201/0.288/0.401 ms

Enter the IP address for ping or [Q/q] to quit this menu:Q
```

Enter *T* to download and install the new image, and the FortiSandbox will reboot automatically.

```

Enter C,R,N,T or Q:t
Connect to http server 10.59.2.148:
  1% [
Image /image/FSA_500F-v300-build0060-FORTINET.out was received.
Format the boot device, then install and launch this firmware? [Y/N]:y
Verifying image sections ... OK
Formatting boot device ... OK
Installing image ... OK
Checking image upgrade stage2 ...done
Booting image .....
Starting FortiSandbox
Check journal on boot device
Initializing core system ...

```

Once successfully booted up, you can log in again with your username and password:

```

Starting FortiSandbox
Check journal on boot device
Initializing core system ...
Detected SN: FSA2KE3117000007
Checking raid settings ...
Initializing hard drive devices ...
Initializing OS components ...
Initializing virtual components ...
Initializing database ...
Initializing scan components ...
Verifying the system ...
Starting system ...

FortiSandbox login: █

```

Retrieving the firmware image from the FTP server

Enter *T* from the main menu to retrieve and upgrade the firmware image from the FTP server.

- Enter *C* to configure the network and image parameters

```

Enter C,R,N,T or Q:c
Available port list: port1 port3
Enter image download port number [port1]:
Enter local IP address [192.168.0.99]:10.59.2.62
Enter local subnet mask [255.255.255.0]:
Enter local gateway [192.168.0.1]:10.59.2.1
Enter DNS [208.91.112.53]:
Enter remote server IP address [192.168.0.199]:10.59.2.148
Enter firmware file name [image.out]:/html/image/image.deb.2000E
Format boot device before install image (Y/N) [N]:y
Enter user name [anonymous]:ftpuser
Enter password [anonymous]:ftpuser
Applying network parameters ... OK

```

Enter *R* to review the parameters.

```

Enter C,R,N,T or Q:r

Image download port: port1
Local IP address: 10.59.2.62
Local subnet mask: 255.255.255.0
Local gateway: 10.59.2.1
DNS: 208.91.112.53
Remote server IP address: 10.59.2.148
Firmware file: /html/image/image.deb.2000E
User name: ftpuser
Password: ftpuser
Format boot device: Y

```


Enter *N* to test the networking.

```
Enter C,R,N,T or Q:n

Enter the IP address for ping or [Q/q] to quit this menu:10.59.2.1
PING 10.59.2.1 (10.59.2.1): 56 data bytes
64 bytes from 10.59.2.1: seq=0 ttl=255 time=0.106 ms
64 bytes from 10.59.2.1: seq=1 ttl=255 time=0.048 ms
64 bytes from 10.59.2.1: seq=2 ttl=255 time=0.045 ms
64 bytes from 10.59.2.1: seq=3 ttl=255 time=0.043 ms
64 bytes from 10.59.2.1: seq=4 ttl=255 time=0.043 ms

--- 10.59.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.043/0.057/0.106 ms

Enter the IP address for ping or [Q/q] to quit this menu:q
```

Enter *T* to download image and install new image, and the FortiSandbox will reboot automatically.

```
Enter C,R,N,T or Q:t

Connect to ftp server 10.59.2.148:
 0% [ ]
Image /html/image/FSA_500F-v300-build0060-FORTINET.out was received.

Format the boot device, then install and launch this firmware? [Y/N]:y

Verifying image sections ... OK
Formatting boot device ... OK
Installing image ... OK

Checking image upgrade stage2 ...done
Booting image .....

Starting FortiSandbox
Check journal on boot device
Initializing core system ...
```

Once successfully booted up, you can log in again with your username and password.

Retrieving the firmware image from a USB drive

Enter *U* to retrieve and upgrade the firmware image from a USB drive.



FortiSandbox VM and KVM products do not support USB options.

Enter *U* to upgrade firmware from a USB drive, and the FortiSandbox will reboot automatically.

```
Enter Q,G,W,T,U,I,F,C or H:u

USB drive(s) with FortiSandbox image:
 device:/dev/sdc version:2 uuid:61589fe0-5917-4e85-8ced-c45f522cab92

please input the device name or [Q/q] to quit the menu:/dev/sdc
Format the boot device before installing new image? [Y/N]:y

Format the boot device, then install and launch this firmware? [Y/N]:y

Verifying image sections ... OK
Formatting boot device ... OK
Installing image ... █
```

Enter *F* to Format device data.

```
Enter Q,G,W,T,U,I,F,C or H:F

The data on the device will be lost after format, do you want to con
tinue?[Y/N]:F

The data on the device will be lost after format, do you want to con
tinue?[Y/N]:y
Preparing device ... Done
Formating device /dev/sda1 ... Done
```



When formatting, all the data on the data device will be lost, such as Windows VMs and log files. After the data device is formatted, installed VMs need to be installed and activated again. Data such as the configuration files on the boot device and the Windows VM license files will not be lost.

Enter */* to show the current system information.

```
Enter Q,G,W,T,U,I,F,C or H:I

CPU model: Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz
CPU flag: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
dpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology
mx smx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic
uid_fault epb cat_l3 cdp_l3 invpcid_single pti intel_ppin tpr_shadow vnmi f
ms invpcid rtm cqm rdt_a rdseed adx smap intel_pt xsaveopt cqm_llc cqm_occu
CPU cores: 24
Memory: 128666 MB
Platform ID: FSA_2000E
Loader Version: V2
Loader Timestamp: 2019-07-19 17:38:51
Loader Mask: Kaa1PEzyxLxZE2udWwV3Fa1MvXxapHVi
Saved Config: v3.1.0,build0106 (Interim)
```

Enter *C* to check the device's file system information.

```
Enter Q,G,W,T,U,I,F,C or H:c

This command would check and repair the filesystem automatically, do you
want to continue?[Y/N]:y
```

a. Enter *B* to check boot device information.

```
Check (B)boot device, (D)data device or (Q) to quit? [B/D/Q]:b
Checking device /dev/sdb:
e2fsck 1.42.7 (21-Jan-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
/lost+found not found. Create? yes

Pass 4: Checking reference counts
Pass 5: Checking group summary information

/dev/sdb1: ***** FILE SYSTEM WAS MODIFIED *****
/dev/sdb1: 125/2560 files (6.4% non-contiguous), 6823/10240 blocks
e2fsck 1.42.7 (21-Jan-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
/lost+found not found. Create? yes

Pass 4: Checking reference counts
Pass 5: Checking group summary information

rescuefmt: ***** FILE SYSTEM WAS MODIFIED *****
rescuefmt: 63/47424 files (19.0% non-contiguous), 173939/189440 blocks
Check process finished.
```

- e. Enter *D* to check data device information.

```
Check (B)boot device, (D)data device or (Q) to quit? [B/D/Q]:d
Preparing device ... Done
Checking device /dev/sda1:
e2fsck 1.42.7 (21-Jan-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
datadisk: 87550/61054976 files (0.6% non-contiguous), 16855633/244190208
blocks

Check process finished.
```

Revalidating Windows license key

FortiSandbox requires reactivating its Windows licenses if the system has been altered. To reactivate, Microsoft has only provided an activation process by phone.

To revalidate and reactivate Windows license key:

1. In FortiSandbox, go to the System Event log to get the installation id and key.
The System Event log lists all failed activation.

2. Search for *Failed to activate*. For example:

```
2021-05-01 13:10:52 VMINIT: WIN7X64VM Windows activation error message:
Failed to activate Windows with key XBBQP-39J47-HFDWW-Y4XJD-XXXXX:
015883135155791636357353814274721005003805545726714080, 0x80072F8F
```

In this example, the installation ID is 015883135155791636357353814274721005003805545726714080 and the key is XBBQP-39J47-HFDWW-Y4XJD-XXXXX.

3. Select a pair of installation ID and key for each failed VM type, and perform the following steps to activate them. You don't need to activate all keys, you only need to activate one key for each failed VM type.
4. Call the Microsoft 24-hour automated system to get a confirmation ID:
Canada/US: 1-888-725-1047
Japan: 0120-801-734
France: 0 805 11 02 35

The automated system will ask you to input the ID (6 characters at a time) and ask some questions about the activation. After that, the system will provide a confirmation ID which will be in a similar format.

5. Go to the FortiSandbox CLI console and use the `confirm-id` command to add the activated ID. For example,

```
confirm-id -a -kGGC2J-Q9M7J-8KKBH-342FP-XXXXX
-c042532258754869596628901610621951021013844450525
```

```
Confirmation ID has been added.
Confirm that the entry have been handle by the FSA :
```

6. Confirm that the ID is activated.

```
confirm-id -l
GGC2J-Q9M7J-8KKBH-342FP-XXXXX 042532258754869596628901610621951021013844450525
```

7. Repeat the above steps to get a confirmation ID and activate it for each failed VM type.
8. To load the activated IDs, reboot your device.

Resetting user's admin password

This procedure requires rebooting the FortiSandbox unit.

You can reset the admin password if you have physical access to the device and the following tools:

- Console cable.
- Terminal software such as Putty.exe (Microsoft Windows) or Terminal (Mac OS X).
- Serial number of the FortiSandbox device.



The new password for the built-in admin is restricted by password policy settings. For more information, see the *FortiSandbox Administration Guide* > [Password Policy](#).

To reset the user's admin password:

1. Connect the computer to the FortiSandbox via the console port on the back of the unit.
2. Start a terminal emulation program on the management computer.
3. Select the COM port and use the following settings:

Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow Control	None

4. Press **Open** to connect to the FortiSandbox CLI.
5. FortiSandbox responds with its name or hostname. If it does not, press **Enter**.
6. Reboot the FortiSandbox using the power button.
7. Wait for the FortiSandbox name and login prompt to appear.
8. Type the username: *maintainer*.
9. The password is *bcpb* + the serial number of the firmware. The letters of the serial number must be in uppercase. You are now connected to the FortiSandbox.
10. To change the admin password, enter the following CLI command:

v3.2.2 and later	<code>reset-admin-pwd</code>
v3.2.0 and earlier	<code>admin-pwd-reset <password_string></code>

11. Log into the FortiSandbox using admin and the password you set in the previous step.



You can disable this maintainer user using the `set-maintainer` command. See the *FortiSandbox CLI Reference Guide* in the [Fortinet Document Library](#).

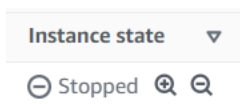
Resizing the data volume on AWS



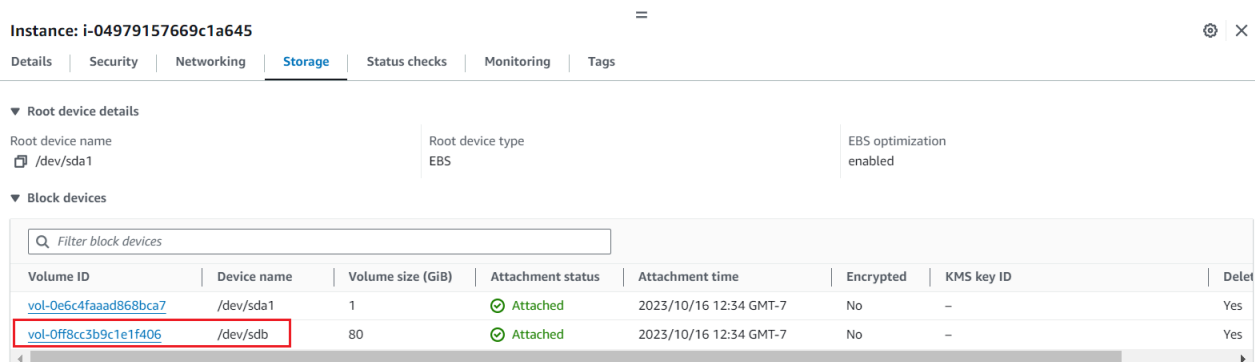
Before proceeding, back up all the data you need as all data is lost in resizing. Resizing without data loss is not currently supported.

To re-size the data volume on AWS:

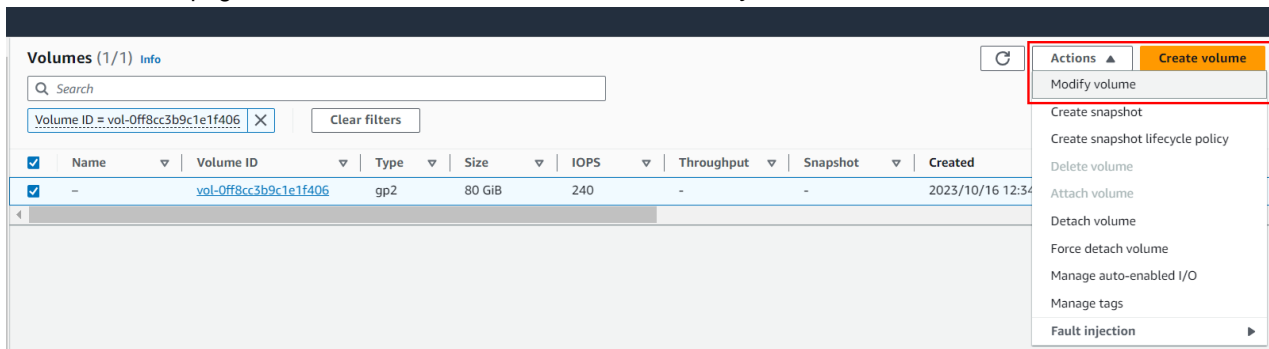
1. Stop the FortiSandbox AWS instance. Ensure the instance is stopped from the AWS EC2 console > Instances.



2. Select the stopped FortiSandbox AWS instance. Click the *Storage* tab. In the *Volume ID* column, click the data volume ID link (located next to the *Device Name*). The *Volumes* page opens.



3. On the *Volumes* page, select the volume, and click *Actions > Modify volume*.



4. Modify the volume details, then click *Modify*.

5. On the confirmation pop-up window, click *Modify* to confirm.

Modify vol-04739a453a1523ea4?

If you are increasing the size of the volume, you must extend the file system to the new size of the volume. You can only do this when the volume enters the optimizing state. For more information see extending the file system for [Linux](#) and [Windows](#).

The modification might take a few minutes to complete.

You are charged for the new volume configuration after volume modification starts. For pricing information, see [Amazon EBS Pricing](#).

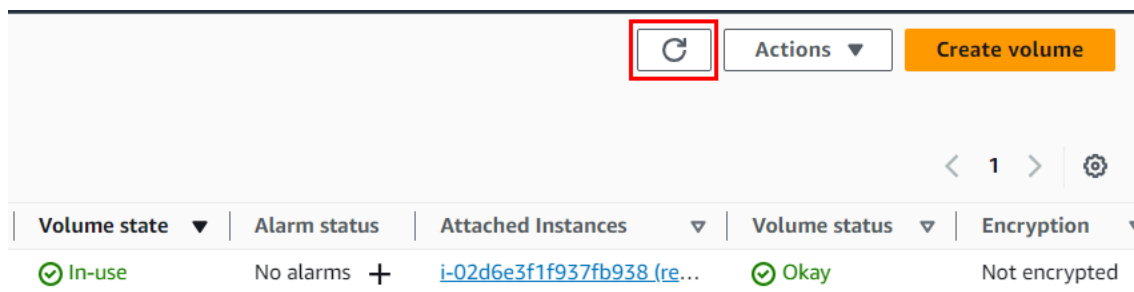
Are you sure that you want to modify vol-04739a453a1523ea4?

Cancel
Modify

6. The AWS EC2 console shows a warning message. This is expected.



7. Click the *Refresh* button next to the *Actions* menu to refresh the page. Ensure the *Volume state* and *Volume Status* are ready to use.



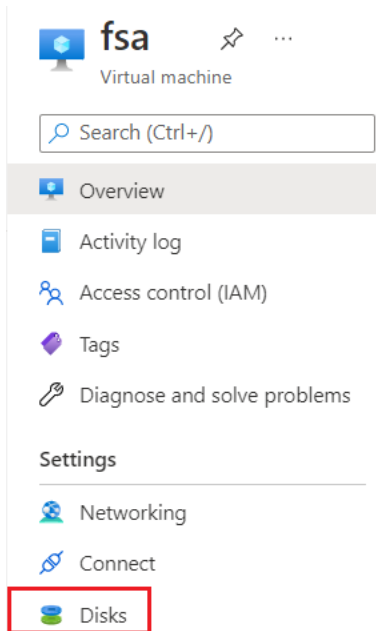
8. Go back to the *Instances* page and start the modified FortiSandbox AWS instance.
9. After FortiSandbox boots up, run the FortiSandbox CLI command: `resize-hd`.
10. After FortiSandbox reboots, run FortiSandbox CLI command: `status` to verify the *Disk Size* is correct.

Resizing the data disk for FortiSandbox on Azure

Use the *Size + performance* settings to maintain the data disk on FortiSandbox on Azure and monitor the disk usage to ensure the data disk does not break.

Scenario 1: Modify FSA data disk without data lost and before disk broken

1. On the Azure Portal, stop the FortiSandbox instance.
2. Go to *FSA Virtual Machine > Overview > Disks > datadisk > Size + performance*.



- Expand Disk SKU and click *Resize*.

_dataDisk | Size + performance

Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Configuration
 - Size + performance**
 - Encryption
 - Networking
 - Disk Export
 - Properties
 - Locks
- Monitoring
 - Metrics
- Automation
 - Tasks (preview)
 - Export template

Disk SKU

Standard HDD (locally-redundant storage)

Size	Disk tier	Provisioned IOPS
32 GiB	S4	500
64 GiB	S6	500
128 GiB	S10	500
256 GiB	S15	500
512 GiB	S20	500
1024 GiB	S30	500
2048 GiB	S40	500
4096 GiB	S50	500
8192 GiB	S60	1300
16384 GiB	S70	2000
32767 GiB	S80	2000

Custom disk size (GiB) *

1024

Resize Discard

- Refresh the Azure Portal and ensure the disk size has been updated.
- On the Azure Portal, start FortiSandbox.

Virtual machine

Search (Ctrl+ /)

Connect Start Restart Stop Capture Delete Refresh Open in mobile CLI / PS Feedback

Overview

Advisor (1 of 3): Management ports of virtual machines should be protected with just-in-time network access control →

- Run the following CLI command: `resize-hd`

```

FSAVM0I000015549> resize-hd
Request to resize hard disk. Resizing will be done during next bootup.
Do you want to continue? (y/n)y
Request has been accepted.
Reboot?
Do you want to continue? (y/n)y
FSAVM0I000015549> Connection to 3.98.189.168 closed by remote host.

```

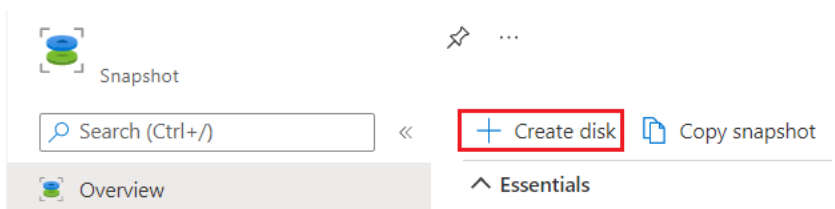
7. After FortiSandbox reboots, run the CLI command `status` to verify the Disk Size is correct.

Scenario 2: Detach/Attach a new FortiSandbox data disk without losing data

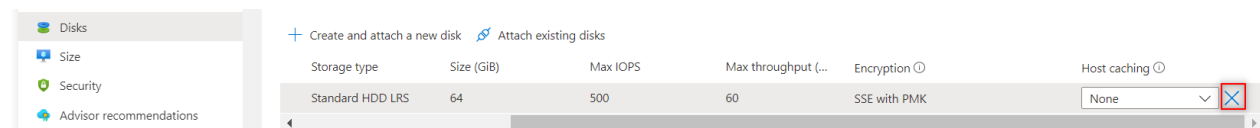
1. On the Azure Portal, stop the FortiSandbox instance.
2. Go to *Data disk > Create snapshot*.



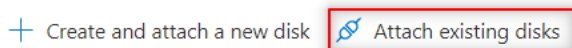
3. Use the snap shot to create a data disk and set the size to 256G or more if needed.



4. Detach the old data disk.



5. Attach the new data disk you created from the snap shot.



6. Refresh the Azure Portal, and confirm the disk has been updated.
 - a. Run the CLI command: `resize-hd`.
 - b. After FortiSandbox reboots use the CLI command `status` to verify the Disk Size is correct.

Setting up a FortiSandbox VM00 as Primary node for high availability

A popular FortiSandbox HA-cluster deployment is based on using FortiSandbox VM00 as a Primary node and one or more FortiSandbox appliances or virtual machines as Worker nodes. A second FortiSandbox VM00 as a Secondary node is highly recommended to make Sandboxing services fault tolerant and configuration simpler.

To set up and operate a healthy and scalable cluster with VM00:

1. H/W Requirements of Primary and Secondary nodes:
 - **Minimum configuration:** Set up the with minimum of: 4 vCPU, 8 GB RAM and 200 GB SSD drive.
 - **Recommended configuration:** 16 vCPU, 32 GB RAM and 1 TB SSD drive.
2. Network Setup:
 - Make sure that network topology, routing and DNS settings of Primary and Secondary nodes are the same.
 - Configure a cluster level failover IP on all ports to provide Sandboxing accessibility (admin-port, api-port, ICAP and MTA/BCC ports).
 - Enable Promiscuous mode in the hypervisor settings (if applicable) to ensure correct operation of failover IP.
3. Configurations on Primary and Secondary nodes;
 - Do not install Windows VMs on these nodes. If these nodes already have them installed, set VM clone number to zero (0)
4. Licenses:
 - Make sure to acquire a *FortiCare Premium Support Only* subscription for the Primary and Secondary nodes configured without any VM Clones. And, make sure to acquire a *Sandbox Threat Intelligence* subscription for all worker nodes.
 - Additional licenses (such as Windows, Office and Custom VM) are only required on nodes with VM Clones configured (i.e. Worker nodes).

Troubleshooting guidelines

The following topics show guidelines on troubleshooting your system.

- [Troubleshooting Dashboard warnings on page 33](#)
- [Troubleshooting system resource issues on page 35](#)
- [Troubleshooting cloning issues on page 36](#)
- [Troubleshooting the Job Queue on page 37](#)
- [Troubleshooting NetShare issues on page 38](#)
- [Troubleshooting detection issues on page 38](#)

Troubleshooting Dashboard warnings

In the *Dashboard*, the color of the *Connectivity and Services* icons indicates their status. When FortiSandbox is fully operational, the icons are green. When FortiSandbox detects a potential issue, the icons are yellow.

Connectivity and Services



This topic provides troubleshooting recommendations for the following services:

- [Windows VM](#)
- [FortiGuard connectivity servers](#)
- [VM Internet access](#)

Windows VM

When Windows VM is initializing, it is normal for the yellow icon to be displayed in the Dashboard. If the yellow icon persists, the Windows VM was not initialized successfully.

To troubleshoot a Windows VM:

Issue	Recommendations	Description
VM image not installed	Go to <i>Scan Policy and Object > VM Settings</i> . Or Run the folling CLI command to display the installed VM images: <code>vm-status -l</code>	Verify that Windows VM images are installed and at least one is enabled and the clone number is not zero.

Issue	Recommendations	Description
Invalid Windows license key	Run the following CLI command: <code>vm-license -l</code>	Check that a Windows 8 image in Optional VMs group is enabled. If not, a valid Windows 8 key should be purchased and installed.
Microsoft server failed to activate	Go to <i>Log & Report > Events > VM Events</i> or <i>All Events</i> .	Verify the logs from the time of the system boot up. For example, errors from Microsoft activation server may help you find the cause of failed activation.

FortiGuard connectivity servers

FortiGuard connectivity servers include FDN update, community cloud, or web filtering.

To troubleshoot connectivity servers:

Issue	Recommendations	Description
Invalid Antivirus DB and Web Filtering Contracts	Go to <i>Dashboard > Status</i> .	Verify Antivirus DB Contract and Web Filtering Contract on Dashboard are valid. If the contracts are valid, the unit may have a bad network connection to external FortiGuard services.
The network is blocking the ping	Run the CLI command: <code>test-network</code>	This can provide detailed information about the network condition. Sometimes the network is blocking the ping and errors about the ping are expected. The output shows connection speed and connectivity to related servers.
Firewall is blocking web filtering query	<ol style="list-style-type: none"> 1. Take the web filtering server IP (available in @@@ testing Web Filtering service @@@ part of test-network command). 2. Go to <i>System > FortiGuard</i>. 3. Use the IP and port 8888 to overwrite the web filtering server. <p>Additionally, enable <i>Use override server port of the community cloud server query</i> and select port 8888 in the <i>Community Cloud & Threat Intelligence Settings</i> section.</p>	Check to see if the firewalls are configured to block packets to UDP port 53. This blocks the web filtering query.

VM Internet access

A yellow icon means the Windows VM cannot access the Internet through port3. This affects the catch rate even if FortiSandbox has a SIMNET feature. For example, the *Downloader* type for malware needs access to an outside network to download a malicious payload.

To verify the VM is using port3 to connect to the Internet:

- Go to *System > Settings > VM External Network Access*.
 - Verify *Allow Virtual Machines to access external network through outgoing port* is enabled.
 - Verify the *Gateway* is valid and can access the Internet.



If no DNS server is set, the system DNS is used.

The screenshot shows the FortiSandbox Settings interface. On the left is a sidebar menu with options like DNS, Static Route, LDAP Servers, SAML SSO, RADIUS Servers, Mail Servers, FortiGuard, Certificates, Login Disclaimer, SNMP, System Recovery, Event Calendar, Event Calendar Settings, Job View Settings, and Settings (highlighted in green). The main content area is divided into two sections. The top section, 'VM External Network Access', has a checkbox 'Allow Virtual Machines to access external network through outgoing port3' which is checked. Below this are fields for 'Status' (with a green checkmark), 'Port3 IP' (with a greyed-out input field), 'Gateway' (with an empty input field), a checkbox 'Disable SIMNET if Virtual Machines are not able to access external network through outgoing port3' which is checked, a 'DNS' field (with an empty input field), and a 'Use Proxy' checkbox which is unchecked. The bottom section, 'Data Storage', has a note 'Clean up schedule. If not set, all job information will be purged after 4 weeks' and a checkbox 'Delete original files of Clean or Other rating after' which is checked. Below this are 'Day (0-27):' and 'Hour:' fields, both with input boxes containing '1' and '0' respectively.

- Run the following command to show network condition through port3.

```
test-network
```

Troubleshooting system resource issues

High CPU or memory usage might indicate a shortage of resources or system-wide issues.

To troubleshoot system issues:

Issue	Recommendation	Description
Increased submissions	Go to <i>Security Fabric > Device</i> .	Check to see if there are any recently-added devices or increases in submissions from devices.

Issue	Recommendation	Description
System configuration	Go to <i>Dashboard > Status > System Information</i> widget.	Check for recently changes to the <i>System Configuration</i> .
System usage	Go to <i>Dashboard > Status > System Resources</i> widget.	Check the CPU, Memory, and Disk Usage reports.
Large pending queue	Go to <i>Scan Job > Job Queue</i> .	Check for large pending jobs. For information, see Troubleshooting the Job Queue on page 37 .
System-wide issues	Run the <code>tac-report</code> CLI command to execute a series of CLI commands for a comprehensive report.	Check the output for possible issues, especially the status and <code>diagnose-sys-top</code> .

If you cannot resolve the issue and you need to contact technical support at <https://support.fortinet.com>, provide the above information to help with troubleshooting.

Troubleshooting cloning issues

This topic provides troubleshooting guidelines when FortiSandbox fails to finish cloning a custom image.

To troubleshoot this issue:

1. Log in as and Admin user.
2. Go to *Scan Policy and Object > VM Settings* and change all other VM types' clone # to 0, and the failed one (customized image) to 1.
3. Click *Apply* to trigger the cloning.
4. Click the *VM Screenshot* button on this page. In the dialog box, keep clicking the *VM Screenshot* button of the failed VM.
5. Click the PNG Link image icon to show the screen shot. The image might provide the reason for the failure.





Common reasons for failure:

Reason	Solution
The custom image is too large for amount the of system memory	<ul style="list-style-type: none"> • Reduce the size of the custom image with Windows Disk Defragmentation tool, or • Reduce the clone number
The customized image license is deactivated	Activate the customized image license.
The system is not configured properly	See the FortiSandbox Cloud Deployment Guide in the Fortinet Document Library.

Reason	Solution
The newer CPU is not compatible with the Hypervisor of the FortiSandbox causing the VM to load slow, show black screen or unable to start.	Contact the Support team to provide a potential hot-fix.

Troubleshooting the Job Queue

When there is a backlog of scans in the *Job Queue* or the jobs have stopped or stalled, the queue may be saturated or the jobs may need to be adjusted.

Input Source	File Type	Queued # 	Ave Scan Time in Last 24 hrs (s)	Expected Finish Time	Arrival Rate (Last 1 hr)	VM Type (Clone #)	 Prioritize
FortiGate	Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF/JS files	63074 		87 Days 14:28:00		WindowsCloudVM(200)	
FortiGate	PDF files	22486 		31 Days 05:32:00		WIN10X64VM(3) 	
Device	Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF/JS files	0	541			WindowsCloudVM(200)	
Device	Microsoft Office files (Word, Excel, PowerPoint files etc)	0	45				
Device	PDF files	0	2772			WIN10X64VM(3) 	
Device	Adobe Flash files	0	17				
Non Sandboxing files	Non Sandboxing files	25534 					
Pending Assignment	Pending Assignment	2 					

To troubleshoot scans in the Job Queue:

Issue	Recommendations	Description
Scan is processing with errors	Go to <i>Log & Report > File statistics > Top File Types widget > Scanned by Sandboxing</i> .	View the logs to check if the scan is still processing with errors. If it is, this usually means most jobs entering the VM and the <i>Scan Profile</i> should be adjusted. The logs can provide clues about which file type should skip sandboxing.
Queue is saturated	Go to <i>Scan Job > Job Queue</i> .	Click the <i>Load Chart</i> of each VM type to see if it is saturated. If it is saturated, allocate a higher clone number to it.
VM errors		View the logs to see if there are VM related errors. VM related errors might mean VM clones are corrupted and cannot be recovered. In this case, the clones need to be rebuilt. To do that, change any clone number in <i>VM Images</i> and click <i>Apply</i> . Wait a few moments and change the clone number back and click <i>Apply</i> again.

If the above does not resolve the issue, you need advanced troubleshooting that require a debug package. Contact technical support at <https://support.fortinet.com>.

Troubleshooting NetShare issues

NetShare issues may occur in older versions of FortiSandbox or when the unit does not have the correct permissions.

To troubleshoot NetShare scan general issues:

1. Ensure you are running version 3.1.1 or above.
2. Check the following:
 - Review the configuration as this is a common error.
 - Check the output of `diagnose-debug netshare` to check the scan process.

NFSv4 error

When Network Share is enabled in NFSv4, the Kernel log may display messages such as *NFS: state manager: check lease failed on NFSv4 server x.x.x.A with error 13*.

In NFSv4, code 13 means *Permission denied. The caller does not have the correct permission to perform the requested operation*.

To troubleshoot this error:

- Check the `/etc/exports` file on the server side to make sure the FortiSandbox unit has the correct permissions for the Network Share folder.

If the above does not resolve the issue, you need advanced troubleshooting that require a debug package. Contact technical support at <https://support.fortinet.com>,

Troubleshooting detection issues

Trace a file

Trace a file to follow the file's route. This is useful when you want to confirm that files are using the route you expect them to take on your network.

To trace a file, you need to know either its checksum or file name.

To trace a file with the checksum:

In the *Log & Report > Events > All Events* page, put the file's checksum or name in the *Message* filter.

Download Log
History Logs
Search

Message

#	Date/Time	Level	User	Message
---	-----------	-------	------	---------

To trace a file with a file within a time-range:

1. In the *Scan Job > File Job Search* page.
2. In the Detection filter, set the time-range and then enter the file's checksum.
3. Click *Show Detail* to show the job's detailed information.

Known malware not detected

If a known malware is not detected, check the following:

Issue	Recommendation	Description
Scan profile	Go to <i>Scan Policy and Object > Scan Profile</i> .	Verify the filter settings have not changed. Check the logs to see if the Scan Profile was changed or a new signature was installed.
Signature or rating engine	Go to <i>System > FortiGuard</i> .	Check to see if a new AntiVirus Signature, Rating Engine, or Tracer Engine was installed.
VM settings	Go to <i>Scan Policy and Object > VM Settings</i> .	The malware might not be able to run in certain VMs.
Network	Go to <i>Log & Report > Network Alerts</i>	View the logs to see if a network condition was changed.
Port3 connection	Go to <i>System > Settings > VM External Network Access</i> .	Check to see if the Port3 connection to the Internet was modified.
Firmware	Go to <i>Dashboard > Status > System Information</i> widget.	Check to see if new firmware was installed.
Execution condition	Go to <i>Scan Policy and Object > Global Network</i> .	If Global Network is enabled, check to see if the malware execution condition was changed, such as down C&C, time bomb, etc.
Verdicts	Go to: <ul style="list-style-type: none"> • <i>Scan Policy and Object > Allowlist/Blocklist</i> • <i>Scan Policy and Object > Yara Rules</i> • <i>Scan Job > Overridden Verdicts</i> • <i>Log & Report > Network Alerts</i> 	Check the logs for any manual overridden verdicts, white/black list, or YARA rule modifications. The Detailed Report in <i>Network Alerts</i> shows how the file was rated. You can also compare the report with a previous version to troubleshoot further.

Issue	Recommendation	Description
Interface	Go to <i>System > Interfaces</i> .	Verify the path for the port3 next hop gateway for the policy is <i>clean</i> .
Other	<ul style="list-style-type: none"> • Try an On-Demand scan of the malware and use the VM Interaction and Scan video features. • Contact Fortinet Support for possible rating/tracer engine bugs. • Report to fsa_submit@fortinet.com for further investigation. 	

Change Log

Date	Change Description
2023-12-05	Updated to version 4.4.3
2023-12-06	Updated Setting up a FortiSandbox VM00 as Primary node for high availability on page 31 .
2023-12-22	Updated Understanding Inline Block feature on page 16 and Hot-swapping hard disk on page 18 .



www.fortinet.com

Copyright© 2024 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 Chief Legal Officer, 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.