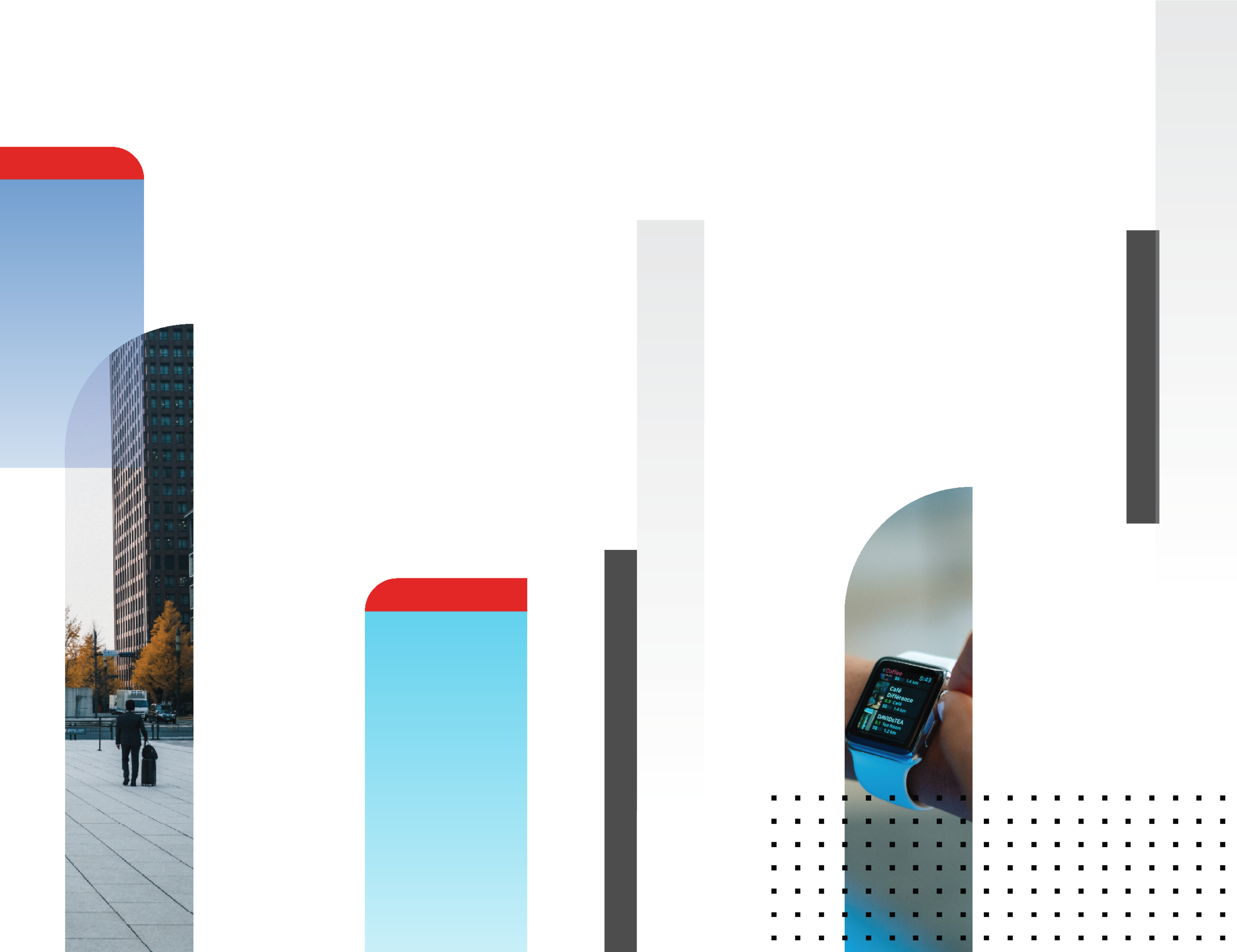
Best Practices and Troubleshooting Guide

FortiSandbox 3.0 and 4.0



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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

July 05, 2021
FortiSandbox 3.0 and 4.0 Best Practices and Troubleshooting Guide
34-40-695977-20210705

TABLE OF CONTENTS

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.

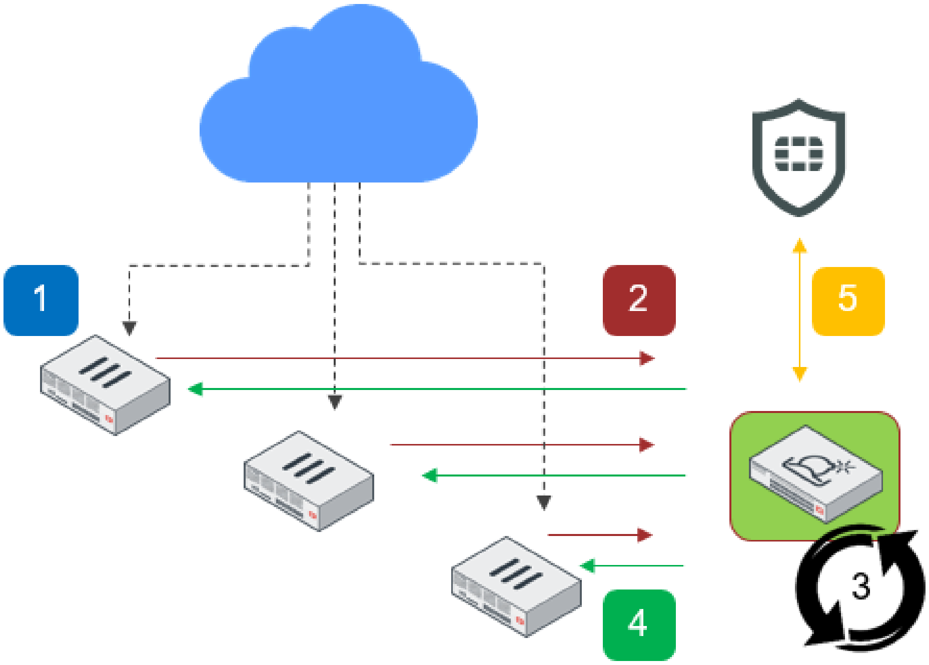
Know your FortiSandbox

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 7. For troubleshooting, see Troubleshooting guidelines on page 24.

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.



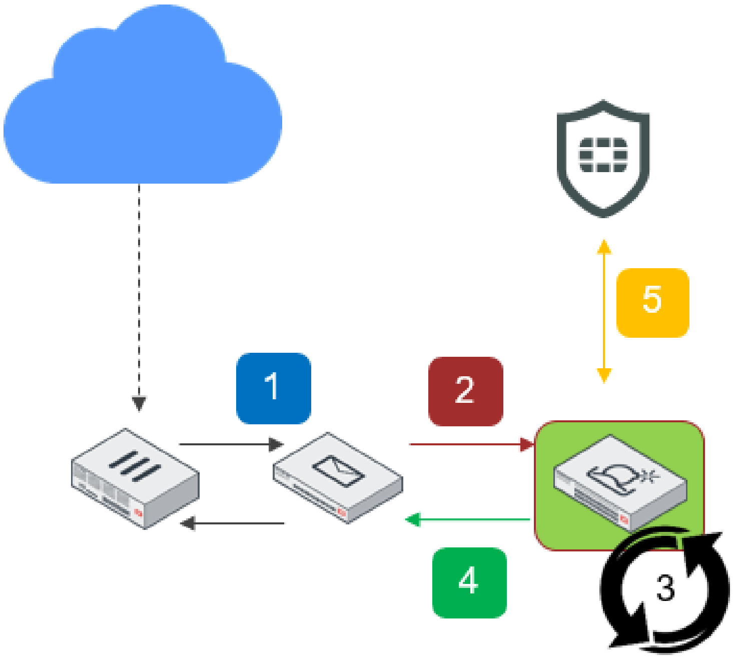
1. FortiGate extracts files from the network traffic. It uses the AntiVirus scan profile for sandboxing feature. File size limit apply. Before forwarding previously seen files, it crosschecks its cache (known as Threat Intelligence DB or Malware package).
2. FortiGate queries FortiSandbox first if previously 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 there is no power interruption. A power loss might damage FortiSandbox databases.
  - Ensure the FortiSandbox environment has a stable and uninterruptible power supply.
  - Always shut down or reboot the FortiSandbox gracefully. Removing power without a graceful shutdown might damage FortiSandbox databases. See Maintaining database integrity on page 9.
- If there is unexpected power loss, revert to a known good backup of the configuration see Restoring the FortiSandbox configuration on page 9.
- 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 *Scan Policy and Object* > *General Settings* to the *Delete all traces of jobs of Clean or Other rating after* setting and set a shorter time period.

Advanced procedures

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

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 *Scan Policy and Object* > *General Settings* and set a short time period in the *Delete all traces of jobs of Clean or Other rating after* section.
2. Turn on FortiGuard 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 FortiGuard Pre-Filtering on some file types. When enabled, files of that file type are inspected by an advanced FortiGuard Pre-Filtering engine and only suspicious files inside a VM are scanned. The *Log & Report* > *File Scan Summary Report* > *Top File Type* > *Scanned by Sandboxing* page 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 image.

   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.

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 default RAID level on different models.

FortiSandbox model	Default RAID Level
FSA-500F	N/A
FSA-1000F/-DC	RAID-1
FSA-2000E	RAID-1
FSA-3000E	RAID-10
FSA-3000F	RAID-10

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

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

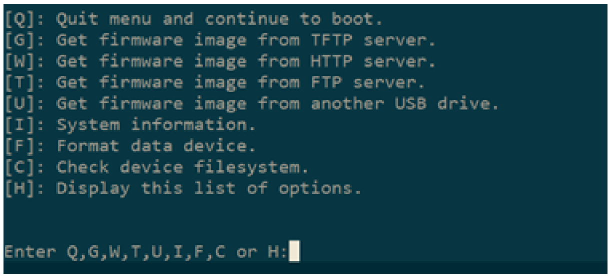
Once a RAID array is built, adding another disk with the same capacity will not affect the array size until you rebuild the array by restarting the FortiSandbox unit.

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:
```

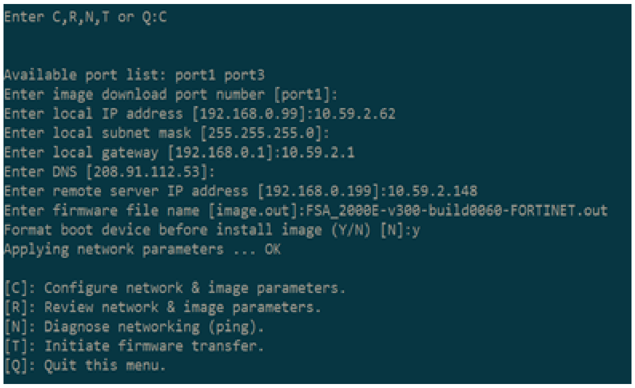
The options are *Q, G,W,T,U,I,F,C* or *H*.

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

Retrieving the firmware image from the TFTP server

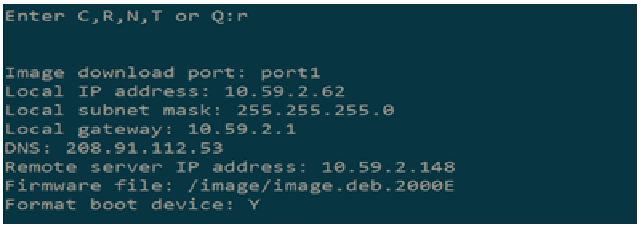
Entering *G* from the main menu will open a sub-menu with options for retrieving and upgrading the firmware image from the TFTP server.

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



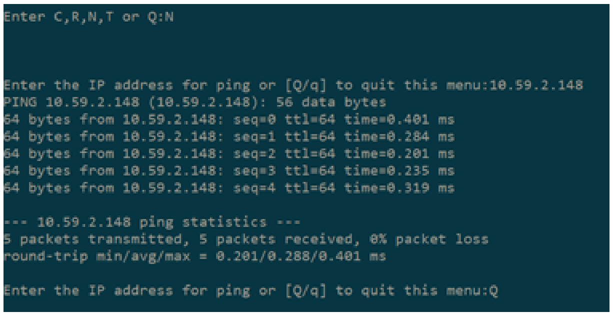
```
Enter C,R,N,T or Q:C


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:



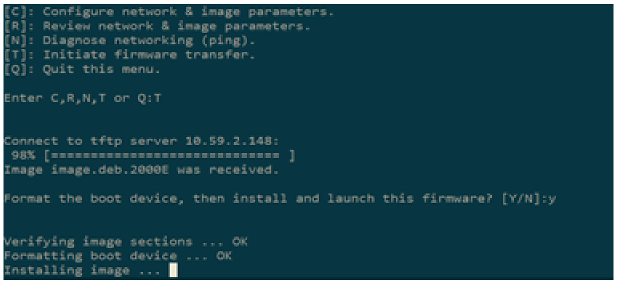
```
Enter C,R,N,T or Q:r


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:



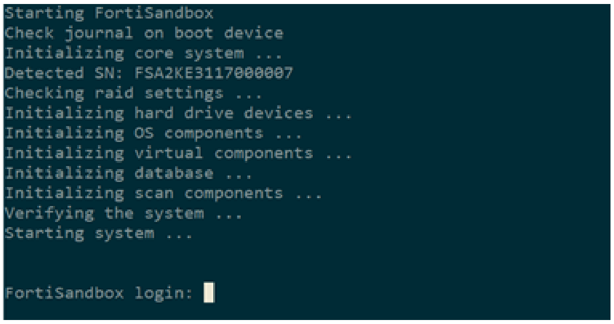
```
Enter C,R,N,T or Q:N



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 theFortiSandbox 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:

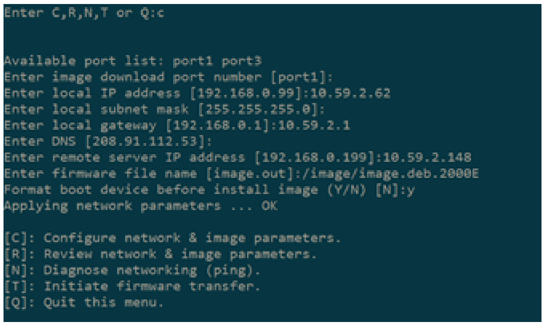


```
Starting FortiSandbox
Check journal on boot device
Initializing core system ...
Detected SN: FSA2KE3117000007
Checking raid settings ...
Initializing hard drive devices ...
Initializing OS components ...
Initializing virtual components ...
Initializing database ...
Initializing scan components ...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


FortiSandbox login: 
```

Retrieving the firmware image from the HTTP server

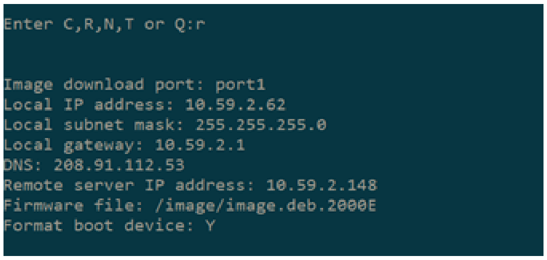
Entering *W* from the main menu will open a sub-menu with options for retrieving and upgrading the firmware image from the HTTP server.

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



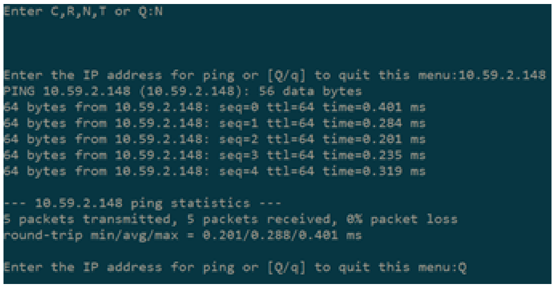
```
Enter C,R,N,T or Q:c


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.



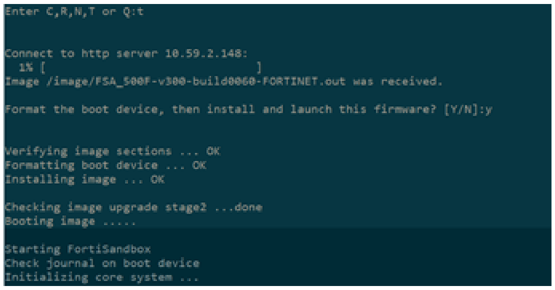
```
Enter C,R,N,T or Q:r


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.



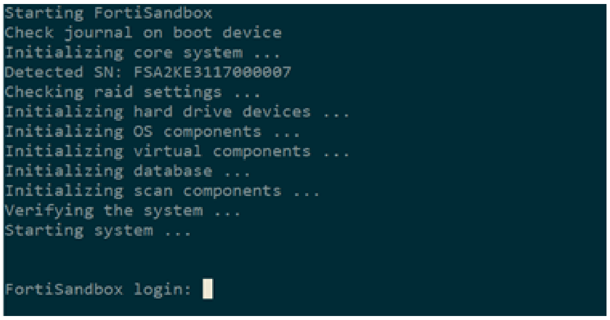
```
Enter C,R,N,T or Q:N



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:

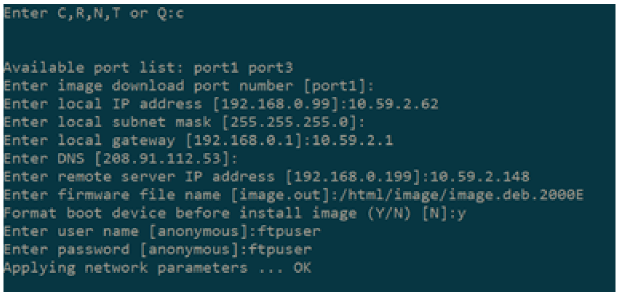


```
Starting FortiSandbox
Check journal on boot device
Initializing core system ...
Detected SN: FSA2KE3117000007
Checking raid settings ...
Initializing hard drive devices ...
Initializing OS components ...
Initializing virtual components ...
Initializing database ...
Initializing scan components ...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


FortiSandbox login:
```

Retrieving the firmware image from the FTP server

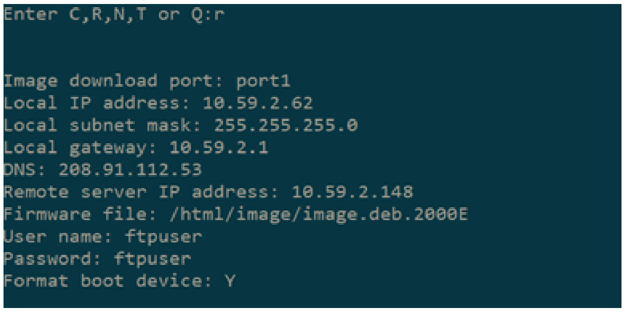
Enter *T* from the main menu to retrieve and upgrade the firmware image from the FTP server.

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



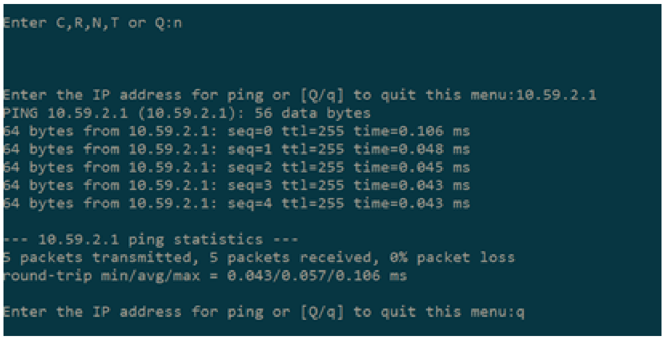
```
Enter C,R,N,T or Q:c


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.



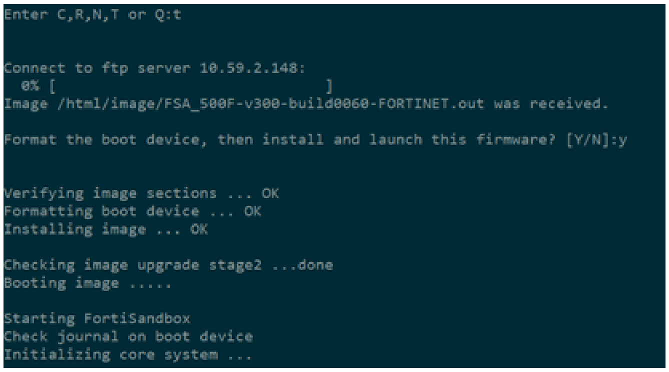
```
Enter C,R,N,T or Q:r


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 ...
```

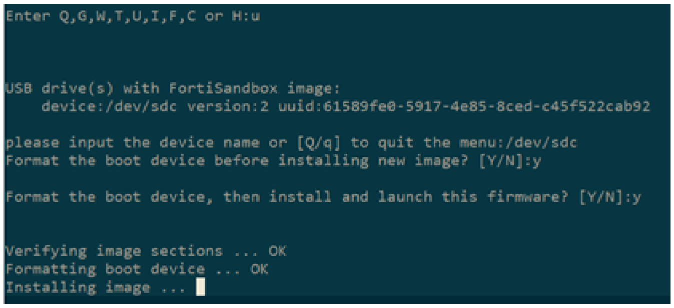
Once successfully booted up, you can log in again with your username and password.

Retrieving the firmware image from a USB drive

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

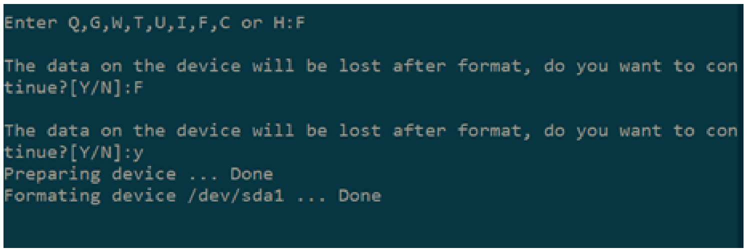
FortiSandbox VM and KVM products do not support USB options.

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 ... 
```

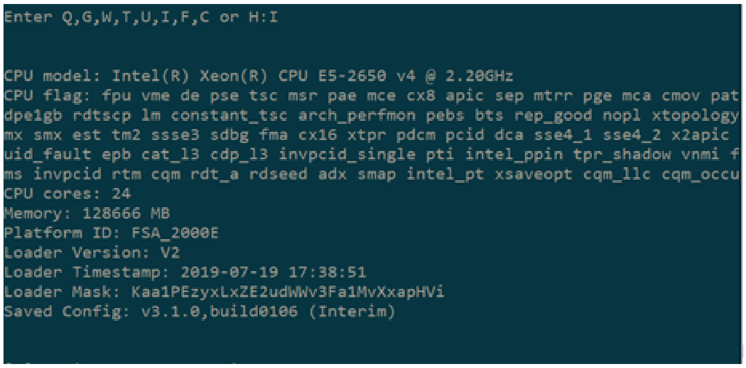
Enter *F* to Format device data.



```
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
```

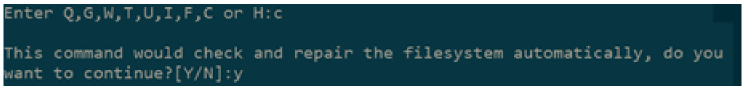
When formatting, all the data on the data device will be lost, such as Windows VMs and log files. After the data device is formatted, installed VMs need to be installed and activated again. Data such as the configuration files on the boot device and the Windows VM license files will not be lost.

Enter *I* to show the current system information.



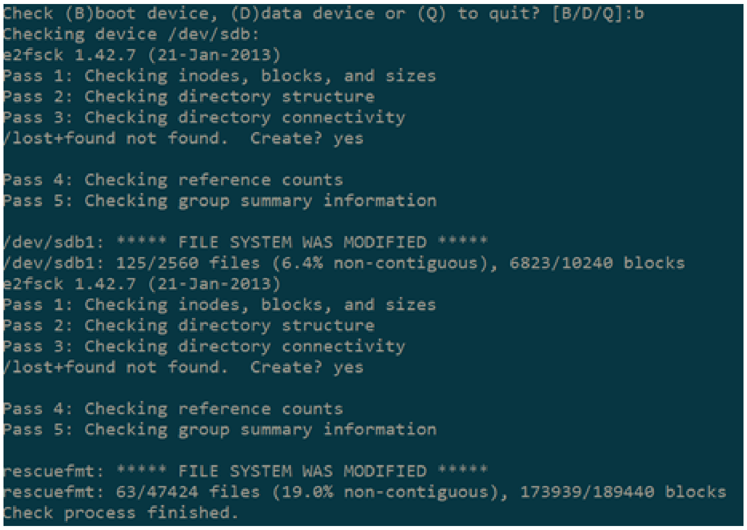
```
Enter Q,G,W,T,U,I,F,C or H:I


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.



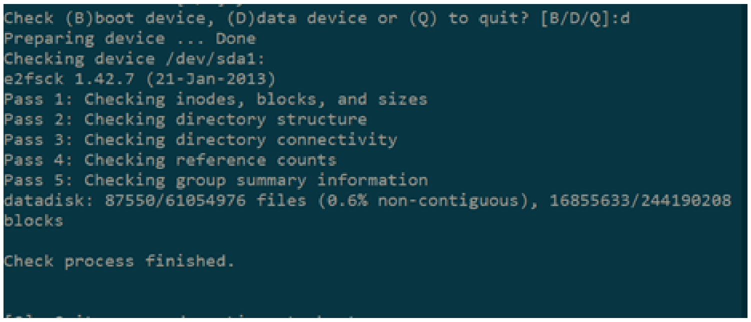
```
Enter Q,G,W,T,U,I,F,C or H:c

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.

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:
    ```
    admin-pwd-reset <password_string>
    ```
11. Log into the FortiSandbox using admin and the password you set in the previous step.

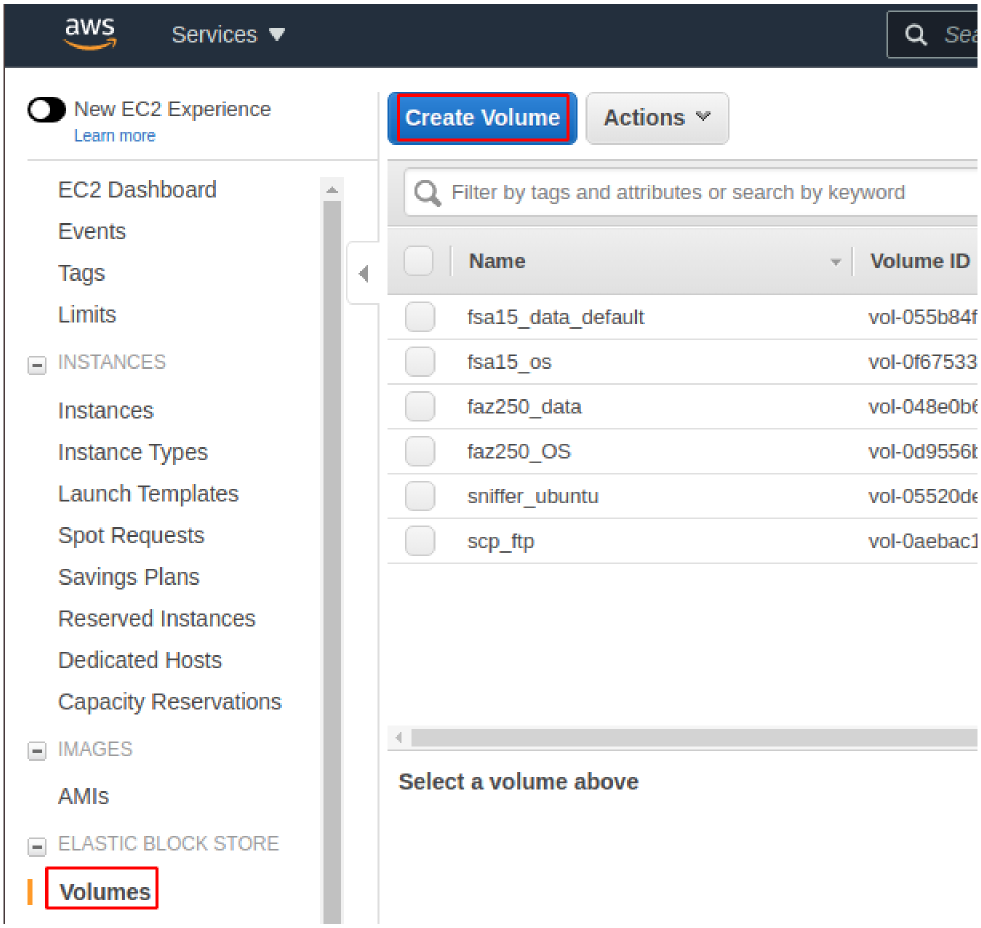
You can disable this maintainer user using the `set-maintainer` command. See the *FortiSandbox CLI Reference Guide* in the Fortinet Document Library.

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.

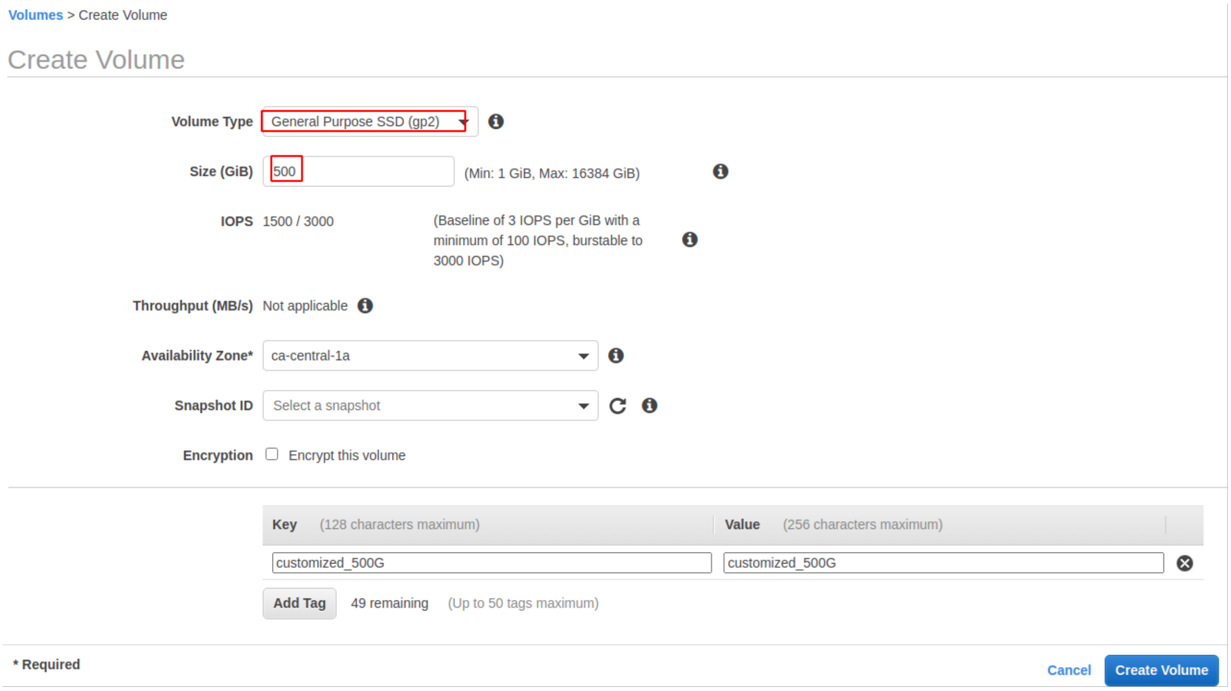
To resize the data volume on AWS:

1. Stop the FortiSandbox AWS instance. Ensure the instance is stopped from the AWS EC2 console.
2. Go to *AWS EC2 console* > *ELASTIC BLOCK STORE* > *Volumes* and click *Create Volume*.



	Name	Volume ID
□	fsa15_data_default	vol-055b84f
□	fsa15_os	vol-0f67533
□	faz250_data	vol-048e0b6
□	faz250_OS	vol-0d9556b
□	sniffer_ubuntu	vol-05520de
□	scp_ftp	vol-0aebac1

3. Specify the volume settings and click *Create Volume*.
   For *Volume Type*, select *General Purpose SSD (gp2)*.
   Enter a *Size (GiB)*.
   If you want, add tags.



Volumes > Create Volume

Create Volume

Volume Type: General Purpose SSD (gp2)

Size (GiB): 500 (Min: 1 GiB, Max: 16384 GiB)

IOPS: 1500 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Throughput (MB/s): Not applicable

Availability Zone*: ca-central-1a

Snapshot ID: Select a snapshot

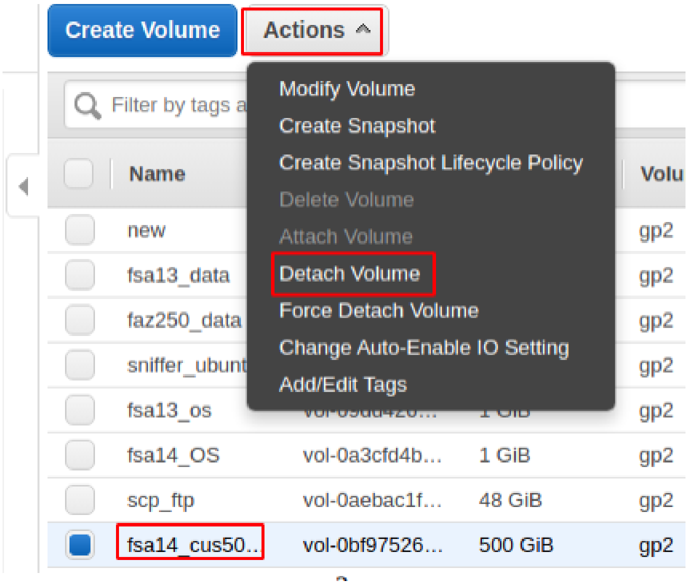
Encryption: □ Encrypt this volume

Key (128 characters maximum)	Value (256 characters maximum)
customized_500G	customized_500G

Add Tag 49 remaining (Up to 50 tags maximum)

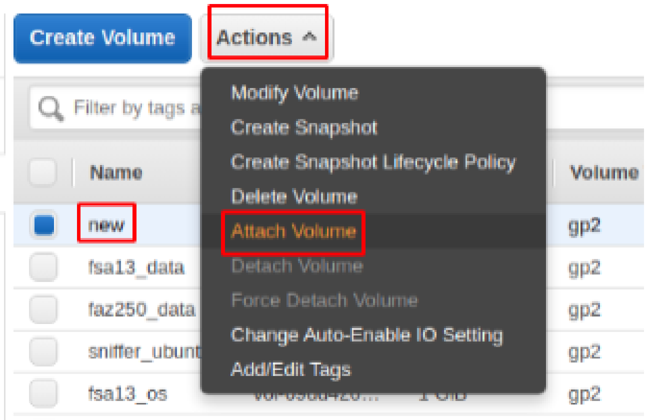
* Required

4. To detach the current FortiSandbox AWS data volume, select the current FortiSandbox AWS data volume and go to *Actions > Detach Volume*.

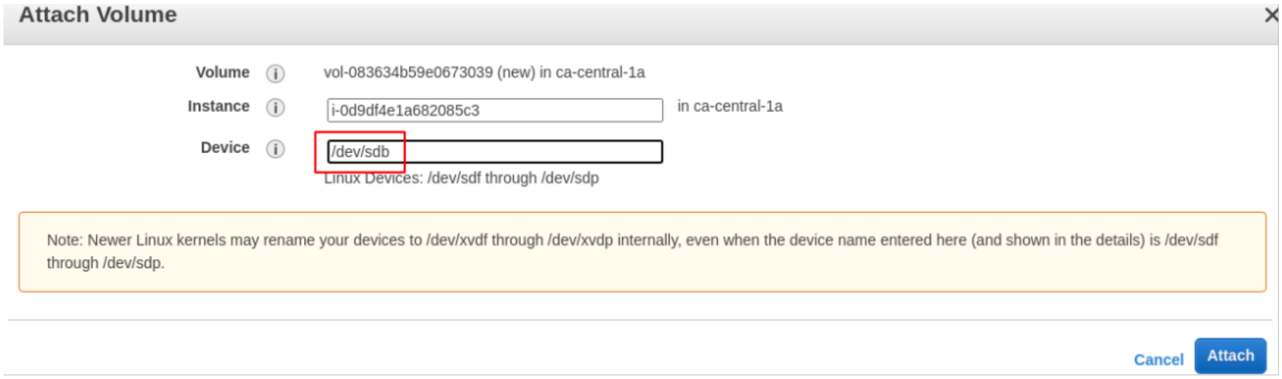


	Name			Volu
□	new			gp2
□	fsa13_data			gp2
□	faz250_data			gp2
□	sniffer_ubunt			gp2
□	fsa13_os	vol-09dd420…	1 GiB	gp2
□	fsa14_OS	vol-0a3cfd4b…	1 GiB	gp2
□	scp_ftp	vol-0aebac1f…	48 GiB	gp2
■	fsa14_cus50..	vol-0bf97526…	500 GiB	gp2

5. Select the volume you just created and go to *Actions* > *Attach Volume*.



6. Select the FortiSandbox AWS instance-ID and in the *Device* field, enter `/dev/sdb`. Then click *Attach*.



Attach Volume

Volume: vol-083634b59e0673039 (new) in ca-central-1a

Instance: i-0d9df4e1a682085c3 in ca-central-1a

Device: /dev/sdb

Linux Devices: /dev/sdf through /dev/sdp

Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

7. Go to *AWS EC2* > *Instances* and select the FortiSandbox AWS instance. In the *Description* on the bottom, go to *Block devices* and select */dev/sdb/*, then check the size of new volume you just attached.
8. Start AWS instance.
9. Run the CLI command `status` and verify that the `Disk Size` is correct.

Troubleshooting guidelines

The following topics show guidelines on troubleshooting your system.

Troubleshooting warning icon in Dashboard

In the Dashboard, the color of the icons indicates status. When FortiSandbox is fully operational, icons are green. Yellow icons indicate that FortiSandbox is seeing a potential issue.

For 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 see initialization details:

1. Go to *Scan Policy and Object* > *VM Settings* and check that there are installed Windows VM images and at least one is enabled (the clone number is not zero). You can also use the CLI command `vm-status -l` to display the installed VM images.
2. Make sure there are valid Windows license keys installed. For example, if Windows 8 image in Optional VMs group is enabled, a valid Windows 8 key should be purchased and installed. Use the CLI command `vm-license -l` to check the Windows keys.
3. Go to *Log & Report* > *Events* > *VM Events* or *All Events* and check the logs from the time of system boot up. For example, errors from Microsoft activation server might help you find the cause of failed activation.

For FortiGuard connectivity servers, such as for FDN update, community cloud, or web filtering

1. Check that Antivirus DB Contract and Web Filtering Contract on Dashboard are valid. If they are, it is possible the unit has a bad network connection to external FortiGuard services.
2. Run the CLI command `test-network`. 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.
3. Some firewalls are configured to block packets to UDP port 53. This blocks web filtering query. To correct this, take the web filtering server IP (available in @@@ *testing Web Filtering service* @@@ part of `test-network` command), go to *System* > *FortiGuard* and use the IP and port 8888 to overwrite the web filtering server. In addition,

enable *Use override server port of community cloud server query* and select *port 8888* in the *FortiSandbox Community Cloud & Threat Intelligence Settings* section.

For VM Internet access

For VM Internet access, it 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 malwares need access to an outside network to download a malicious payload.

To rectify, check the following:

1. In the *Scan Policy and Object > General Settings* page, check that *Allow Virtual Machines to access external network through outgoing port* is enabled.
2. A valid Gateway should be provided. The gateway should be able to access the Internet. If no DNS server is set, the system one is used.
3. Use the CLI command `test-network` to show network condition through port3.

Troubleshooting high system utilization

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

If your system has high CPU or memory usage, check the following:

- Are there any recently-added devices or increases in submissions from devices.
- Did you recently change the system configuration.
- Check the Dashboard for system usage and other indicators.
- In the *Scan Jobs* GUI, check the *Large Pending Queue* section.
- Run the `tac-report` CLI command to execute a series of CLI commands for a comprehensive report. Check the output for possible issues, especially the status and `diagnose-sys-top`.

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.

Tracing a file

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

To trace a file:

1. In the *Log & Report > Events > All Events* page, put the file’s checksum or name in the *Message Filter*.
2. In the *Scan Job > File Job Search* page, search the file’s checksum or name within a time-range. Then click *Show Detail* to show the job’s detailed information.

Cloning custom image does not finish

To troubleshoot this issue:

1. Login as user with admin rights.
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*. This triggers 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. Then click the PNG Link image icon to show the screenshot. The image might provide the reason for the failure.

Common reasons for the failure:

1. The custom image is too large so that the system does not have enough memory. Possible solutions are to reduce its size with Windows Disk Defragmentation tool or reduce clone number.
2. The customized image license is inactivated.
3. The system is not configured properly. See the VM guide in the Fortinet Document Library.

Troubleshooting long pending queue

If you have a long pending queue and the scan is not processing or processing slowly, check the following:

1. View the logs to check if the scan is still processing with errors. If it is, it usually means most jobs entered VM and the Scan Profile should be adjusted.
   Log & Report > *File Scan Summary Report* > *Top File Type* > *Scanned by Sandboxing* can give you hints about which file type should skip sandboxing.
2. You can also go to *Scan Input* > *Job Queue* to see which is the longest queue. Click *Load Chart* of each VM type to see if it is saturated. If it is saturated, allocate a higher clone # to it.
3. 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 *VM Images* and click *Apply*. Wait a few moments and change the clone number back and click *Apply* 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 scan issues

To troubleshoot NetShare scan issues, first ensure you are running version 3.1.1 or above. Next, check the following:

- Re-check the configuration as this is a common pitfall.
- Check the output of `diagnose-debug netshare` to check the scan process.

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 undetected known malware

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

- Scan profile was changed. The malware might not be able to run in certain VMs.
- A new AV/IPS signature, rating engine, tracer engine was installed.
- Network condition was changed.
- Port3 connection to Internet was modified.
- New firmware was installed.
- The malware execution condition was changed, such as down C&C, time bomb, etc.

The following are some troubleshooting methods:

1. Check the logs to see if the Scan Profile was changed or a new signature was installed.
2. Check logs for any manual overridden verdicts, white/black list, or YARA rule modifications. The Detailed Report shows how the file was rated.
3. Run `test-networks` to see unit connection to FDN, especially if Web Filter service is down.
4. Check port3 next hop gateway for the policy. The path should be *clean*.
5. Try an On-Demand scan of the malware and use the VM Interaction and Scan video features.
6. Compare a previous Detailed Report with a recent one.
7. Contact Fortinet Support for possible rating/tracer engine bugs.
8. Report to fsa_submit@fortinet.com for further investigation.

Change Log

Date	Change Description
2021-04-19	Initial release.
2021-05-05	Updated Revalidating Windows license key on page 19.
2021-07-05	Added Maintaining storage integrity on page 10 and Resizing the data volume on AWS on page 21.

www.fortinet.com