CLI Reference Guide

FortiSandbox 5.2.0

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

June 8, 2026
FortiSandbox 5.2.0 CLI Reference Guide
34-520-1194117-20250608

TABLE OF CONTENTS

Introduction

You can access the FortiSandbox CLI (Command Line Interface) using the FortiSandbox console or using an SSH or TELNET client. These services must be enabled on the port1 interface.

CLI commands are intended to be used for initial device configuration and troubleshooting. Some commands are specific to hardware or VM devices. Use `?` or `help` with the command for information on how to use the command.

An administrator's privilege to execute CLI commands is defined in the admin profile. In the admin profile, enable the `JSON API / CLI` option to allow administrators with that profile to execute all CLI commands. Disabling that option restricts administrators with that profile to a limited subset of CLI commands.

The FortiSandbox CLI is case-sensitive.

General

Command	Description
`?`	Synonym for `help`.
`exit`	Exit from the CLI.
`help`	Display this text.

Configuration commands

The following configuration commands are available:

Command	Description
`set`	Set configuration parameters.
`show`	Show the bootstrap configuration, including the port IP address (IPv4 and IPv6), network mask, port MAC address, and default gateway. If the port is being used by a sniffer, it will not be displayed.
`unset`	Unset the admin port or the default gateway.

set

Set configuration parameters.

Syntax

```
set <admin-port>
set <api-port>
set <date>
set <default-gw>
set <port3-speed> <auto|<speed {full|half}]
set <port-mtu> <portx> <1200-9000>
set <portX-ip> <ip/netmask>
set <time>
```

Attribute	Value	Description	Example
`admin-port`	`portx`	Enable a new administrative port other than port1. This cannot be set to port3 or sniffer ports.	`admin-port port2`
`api-port`	`portx`	Set ports for API connection.	`api-port port2`
`date`	`date`	Set system date, in the format of YYYY-MM-DD.	`date 2023-10-31`
`default-gw`	`ip`	Set the default gateway address.	`default-gw 1.2.3.4`

Attribute	Value	Description	Example
port3-speed	auto speed {full|half}	Set port3 speed and duplex settings. This attribute is not supported on VM models or 3000G. All NICs in the 3000G have been upgraded to 10G transceiver NICs, which do not allow speed changes.	port3-speed 1000 full, port3-speed auto
port-mtu	<portx> <1200-9000>	Set a port's MTU value.	port-mtu port1 1200
portX-ip	<ip/netmask>	Set the portX IP address in IP/netmask format. This can also set the address on aggregate ports.	port1-ip 1.2.3.4/24 port2-ip 1.2.3.4/24
time	<time>	Set system time, in the format of HH:MM:SS.	time 12:00:00

show

Show the bootstrap configuration, including the port IP address (IPv4 and IPv6), network mask, port MAC address, and default gateway. If the port is being used by a sniffer, it will not be displayed.

Syntax

```
show
```

unset

Unset the admin port or the default gateway.

Syntax

```
unset admin-port
unset api-port
unset default-gw
```

Diagnose commands

The following diagnostic commands are available:

Command	Description
`diagnose-clilog`	Record all CLI input and output.
`diagnose-debug`	Display detailed debug logs of network share scan and communications with devices.
`diagnose-krnlog`	Record the kernel ring buffer.
`diagnose-sys-perf`	Display system performance information.
`diagnose-sys-top`	Display system top information.
`disk-attributes`	Display system disk attributes. This option is only available on hardware models.
`disk-errors`	Display any system disk errors. This option is only available on hardware models.
`disk-health`	Display disk health information. This option is only available on hardware models.
`disk-info`	Display disk hardware status information. This option is only available on hardware models.
`hardware-info`	Display general hardware status information. Use this option to view CPU, memory, disk, and RAID information, as well as system time settings, and hardware temperature, fan speed, Power Supply Status and hard-disk status.
`raid-hwinfo`	Display RAID hardware status information, including if auto RAID (AutoRebuild) is enabled. This option is only available on hardware models.
`redis-info`	Display Redis memory usage and key information.
`tac-report`	A collection of configuration, diagnostic, system, and utility commands for monitoring and troubleshooting purposes.

diagnose-clilog

Record and display CLI inputs and outputs.

Syntax

```
diagnose-clilog [-h|-e|-d|-l|-s]
```

Option	Description
-h (or --help)	Show help.
-e	Enable recording CLI logs.
-d	Disable recording CLI logs (default).
-l	List the current CLI log recording status.
-s	Show recorded CLI logs.

diagnose-debug

Display detailed debug logs of network share scan and communications with devices. It is useful for troubleshooting OFTP and network share scan issues.

Syntax

```
diagnose-debug [netshare|device|adapter|anti-phishing|inline-block|android|vminit|fdn|disk
      usage|report]
```

Option	Description
netshare	Network share daemon
device	OFTP daemon for FGT/FML/FCT devices
adapter_icap	Daemon for Internet Content Adaptation Protocol (ICAP)
adapter_bcc	Daemon for BCC
adapter_mta_relay	Daemon for MTA Relay
adapter_mta_list	Pending emails for MTA Sending
anti-phishing	Real-time Zero-Day Anti-Phishing Service
inline-block	Inline block for devices

Option	Description
android	Android vm scan
vminit	VM init
fdn	FDN update
disk-usage	Show disk usage statistics for VMs and jobs
report	Show the report generating process

diagnose-krnlog

Record and display kernel logs.

Syntax

```
diagnose-krnlog [-h|-e|-d|-l|-s]
```

Option	Description
-h (or --help)	Show help.
-e	Enable recording kernel log.
-d	Disable recording kernel log (default).
-l	List the current kernel log recording status.
-s	Show the recorded kernel log contents.

diagnose-sys-perf

Display system performance information.

Syntax

```
diag-sys-perf -[h|m<hours>]
```

Optionally, you can specify how many previous hours to show with -m<hours> (maximum = 672, default = 1).

Option	Description
-h (or --help)	Help information.

Option	Description
-m<hours>	Optional) Specify how many previous hours to show (maximum = 672, default= 1).

diagnose-sys-top

Display current system top processes and current CPU and memory usage.

Syntax

```
diagnose-sys-top [-h|l|i]
```

Option	Description
-h (or --help)	Help information.
-l<value>	Maximum lines (maximum = 100, default = 50).
-i<value>	Interval to delay, in seconds (default = 5).

Keyboard input operations:

q	or ^C to quit.
m	Sort by memory usage.
p	Sort by CPU usage
t	Sort by time usage.
n	Sort by PID

disk-attributes

Display system disk attributes. This option is only available on hardware models.

Syntax

```
disk-attributes
```

disk-errors

Display any system disk errors. This option is only available on hardware models.

Syntax

```
disk-errors
```

disk-health

Display disk health information. This option is only available on hardware models.

Sytnax

```
disk-health
```

disk-info

Display disk hardware status information. This option is only available on hardware models.

Syntax

```
disk-info
```

hardware-info

Display general hardware status information. Use this option to view CPU, memory, disk, and RAID information, as well as system time settings, and hardware temperature, fan speed, Power Supply Status, hard-disk status. In addition, the G-model also provides TPM2 and PCI information.

Syntax

```
hardware-info
```

raid-hwinfo

Display RAID hardware status information, including if auto RAID (AutoRebuild) is enabled. This option is only available on hardware models.

Syntax

```
raid-hwinfo
```

redis-info

Display Redis memory usage and key information.

Syntax

```
redis-info
```

Example:

```
### Total System Memory

    31.36G

### Redis Memory Usage

Firmware Redis Memory Usage: 1.36M
Firmware Redis Peak Memory Usage: 1.47M
Firmware Redis Max Memory: 15.31G

# Firmware Redis Keyspace
db0:keys=199,expires=179,avg_ttl=408342296
db1:keys=5,expires=5,avg_ttl=349808215

Engine Redis Memory Usage: 1.82M
Engine Redis Peak Memory Usage: 2.46M
Engine Redis Max Memory: 15.31G

# Engine Redis Keyspace
db0:keys=3,expires=0,avg_ttl=0
db3:keys=4,expires=0,avg_ttl=0
db4:keys=4,expires=0,avg_ttl=0
```

tac-report

The Technical Assistance Center (TAC) report runs an exhaustive series of diagnostic commands. Fortinet support may ask you to use the report output to provide information about the current state of your FortiSandbox. Due to the amount of output generated, the report may take a few minutes to run.

Syntax

```
tac-report [-h}
```

Option	Description
-h	Help information.

Sample output

Tac-report Includes a section for output of *hc-status -l*

To interrupt the output of the `tac-report` command, press `Ctrl+C` twice.

Standalone unit

This unit is in standalone mode:

```
### Display HA-Cluster information ################################################
```

This unit is in standalone mode:

```
### Display HA-Cluster all units information ######################################
```

Primary

```
### Display HA-Cluster information ################################################


SN: FSAVM0TM23002064
Type: Primary
Name: MasterA
HC-Name: EZCluster
Authentication Code: pass
Interface: port2
Cluster Interfaces:
        port1: 10.59.26.250/24
Encryption: Disabled
```

```
### Display HA-Cluster all units information ######################################
```

```
Status for all units in cluster: EZCluster
-------------------------------------------------------------------------------
SN                  Type           Name                IP                  Active
FSAVM0TM23002064    Primary        MasterA             44.44.1.235         1 second ago (0 in
processing, 2 clones)
FSAVM0TM21090029    Secondary      PslaveB233          44.44.1.233         1 second(s) ago (0
in processing, 1 clones)
```

Secondary

```
### Display HA-Cluster information ################################################


SN: FSAVM0TM21090029
Type: Secondary
Name: PslaveB233
HC-Name: EZCluster
Authentication Code: pass
Interface: port2
Encryption: Disabled

### Display HA-Cluster all units information ######################################


Status of primary and secondary units in cluster: EZCluster
-------------------------------------------------------------------------------
SN                  Type           Name                IP                  Active
FSAVM0TM23002064    Primary        MasterA             44.44.1.235         1 second(s) ago
FSAVM0TM21090029    Secondary      PslaveB233          44.44.1.233         1 second(s) ago
```

Worker

```
### Display HA-Cluster information ################################################


SN: FSAVM0TM21090029
Type: Worker
Name: Worker
HC-Name: EZCluster
Authentication Code: pass
Interface: port2
Encryption: Disabled

### Display HA-Cluster all units information ######################################


Status of primary and secondary units in cluster: EZCluster
-------------------------------------------------------------------------------
SN                  Type           Name                IP                  Active
FSAVM0TM23002064    Primary        MasterA             44.44.1.235         1 second(s) ago
```

Monitoring and troubleshooting

The following monitoring and troubleshooting commands are available:

test-network

Test the network connection. The output can be used to detect network speed and connection to FDN servers and the Internet.

Syntax

```
test-network [option]
```

Option	Description
h (or --help)	Help information.
[Connectivity]	
connect	Test system Internet connection
aws_connection	Test AWS config connection and ping for AWS via port1 and port2
azr_connection	Test Azure config connection and ping for Azure via port1 and port2
gcp_connection	Test GCP config connection and ping for GCP via port1 and port2
faz_connection	Test FortiAnalyzer server connection
fndr_connection	Test FortiNDR service endpoint
local_resolve_speed	Test system DNS resolve
ping_speed	Test ping speed
resolve_speed	Test VM DNS resolve speed
vm_connect	Test VM instances Internet access or URL content check via port3
wget_speed	Test wget speed
[FortiGuard Services]	
anti_phishing	Test Real-time Zero-Day Anti-Phishing Service server connection.
cloudvm	Test FSA Dynamic Scan (Cloud) VM service
fdn	Test FDN service

Option	Description
fortiguard_upload	Test statistics data submission to fortiguard service status
macvm	Test FSA Dynamic Scan (MacOS Cloud) VM service
rating_service_endpoint	Test Cloud Rating
sandbox_community	Test Sandbox Community Cloud service
sandbox_community_upload	Test sandbox community cloud submission status
vm_downloadable	Test VM downloadable
web_filter	Test Web Filtering service
webfilter_upload	Test webfilter service submission status

HA Cluster

The following HA Cluster commands are available:

Command	Description
hc-primary on page 20	Configure the unit as a HA-Cluster primary unit.
hc-settings on page 21	Configure the unit as a HA-Cluster mode unit.
hc-status on page 22	This CLI is used to check HA-Cluster status. For all the units in a cluster, the command will display the SN, the unit type, the name in cluster, the IP inside cluster, and the status of active.
hc-worker on page 23	Configure the unit as a HA-Cluster worker or secondary unit.

hc-primary

Configure the unit as a HA-Cluster primary unit.

syntax

```
hc-primary [-h|-l|-r|-sg|-u|-s|-e|-d|-si|-i|-a|-r|-so|-a|-p|-m]
```

Option	Description
-h (or --help)	Help information.
-l	Show current configuration.
-r <unit sn>	Remove a secondary or worker unit from the cluster by its serial number.
-sg	General settings.

Option	Description
-u	Turn off file scans on the primary unit.
-s<10-100>	Turn on file scans on the primary unit with 10%–100% processing capacity.
-e	Enable encrypted traffic between HA cluster

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>members.</td></tr>
<tr><td>-d</td><td>Disable encrypted traffic between HA cluster members.</td></tr>
</table>
</td></tr>
<tr><td>-si</td><td>Configure external IP addresses for the cluster.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-i <interface></td><td>Specify the interface used for external communication.</td></tr>
<tr><td>-a <IP/netmask></td><td>Add an external IP address to the specified interface. The IP will be configured as an alias IP and must be in the same subnet as the interface IP.</td></tr>
<tr><td>-r <IP/netmask></td><td>Remove an external IP address from the specified interface.</td></tr>
</table>
</td></tr>
<tr><td>-so</td><td>Set/Unset HA mode of the cluster (Available on Primary only).
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-a</td><td>Set Primary and Secondary units to Active-Active mode.</td></tr>
<tr><td>-p</td><td>Set Primary and Secondary units to Active-Passive mode.</td></tr>
<tr><td>-m</td><td>Set Primary and Secondary units to Cluster Management mode</td></tr>
</table>
</td></tr>
</table>

hc-settings

Configure the unit as a HA-Cluster mode unit.

syntax

```
hc-settings [-h|-l|-sc|-t|-n|-c|-p|-i|-m]
```

Option	Description
-h (or --help)	Display help information.

Option	Description
-l	Show current HA cluster configuration.
-sc	Add this unit to an HA cluster.

Option	Description
-t<N|M|P|R>	Set the role of this unit in the HA cluster as: N Standalone unit. M Primary unit. P Secondary unit. R Worker unit.
-n<name>	Set alias name of the unit.
-c<cluster-name>	When the unit is operating as the Primary node, set the HA cluster name. This name is used for validation when configuring other unit types.
-p<auth-code>	When the unit is operating as the Primary node, set the HA cluster authentication code. This code is used for validation when configuring other unit types.
-i<interface>	Specify the interface for cluster internal communication.
-m	Join the cluster as a Cluster Management unit (Primary and Secondary units only). If the unit does not have a tracer or rating engine installed, this option is mandatory, and the unit will operate in Cluster Management mode.

Example

```
hc-settings -sc -tM -nPrimay -cClusterTest -p123abc -iport2
```

hc-status

This CLI is used to check HA-Cluster status. For all the units in a cluster, the command will display the SN, the unit type, the name in cluster, the IP inside cluster, and the status of active.

syntax

```
hc-status [-h|-l]
```

Option	Description
-h (or --help)	Help information.
-l	List the status of HA-Cluster units.

hc-worker

Configure the unit as a HA-Cluster worker or secondary unit.

syntax

```
hc-worker [-h|-a|-r|-u|-s|-p]
```

Option	Description
-h (or --help)	Help information.
-a	Add the worker/secondary unit to the HA-Cluster.
-r	Remove the worker/secondary unit from the HA-Cluster.
-u	Update the worker/secondary unit information.
-s	The primary unit IP address.
-p	The HA-Cluster authentication code.

Example

```
hc-worker -a -s10.0.2.5 -p1111
```

Scan

The following scan commands are available:

device-clean-pdf on page 25	FortiSandbox will send job detail PDF to FortiGate when requested. You can decide whether a template PDF or the actual job detail PDF will be sent for clean jobs. For malicious/suspicious files, the actual job detail pdf will always be sent to FortiGate. By default, for clean jobs, FortiSandbox will only send a template PDF.
filesize-limit on page 25	Set the maximum single file size and the maximum child file size to scan.
fortimail-expired on page 26	Enable/disable timeout check for FortiMail files. By default, FortiMail will hold mail for set period to wait for the verdict from FortiSandbox. Before FortiSandbox scans a file or URL that is sent from FortiMail, it will check if the verdict is still needed - FortiMail may have already released the email after timeout. If not, FortiSandbox will give the job an Other rating and a skipped status.
inline-block-timeout on page 27	Set the timeout value to replay the request from FortiOS.
paix-ioc	Enable static IOC enhancement.
pending-jobs on page 28	This command allows users to view job queues statistics and purge them.
prescan-config on page 29	Configure support for large files of up to 10GB in VM. Large file support is only available for VMs although this command is available on all platforms. Large files are usually archive files that contain many files.
processing-jobs on page 30	Use this command to display or purge the jobs in process. After canceling the jobs in processing, the job status is shown as Canceled in the job details.
sandboxing-adaptive on page 31	Turn adaptive scan on or off.
sandboxing-embeddedobj	Turn on or off sandboxing embedded URLs or QR code, image or executable file in documents. A maximum of three randomly selected URLs will be scanned inside the VM if sandboxing is enabled, with unrated URLs taking priority over those that are already rated if the prefilter is enabled.
sandboxing-parallel on page 32	Turn parallel scan on or off.
sandboxing-pipeline on page 33	Pipleline Mode improves performance and accelerate the scan by reducing the time spent on VM instance starts and shutdowns. This allows jobs to be scanned in a VM instance one by one without shutting down the instance.
sandboxing-prefilter on page 33	Allow user to turn FortiGuard prefiltering on or off for certain file types.

sandboxing-ratio on page 34	Turn VM scan ratio on or off.
sandboxing-rse on page 35	Turn rating service endpoint API on or off. When off, FortiSandbox uses local rating source. When on, FortiSandbox uses it as the rating source only when the results returned by the rating service are different from the results from local rating.
scan-perf	Retrieve system scan performance statistics, including both static and dynamic scans, for up to the past 28 days.
url-deep-check	Use this command to view, configure, and control advanced URL inspection features that analyze URLs for potential security threats.
url-recheck on page 36	Enable/disable trusting previous scan results in Fortimail URL scan.

device-clean-pdf

FortiSandbox will send job detail PDF to FortiGate when requested. You can decide whether a template PDF or the actual job detail PDF will be sent for clean jobs. For malicious/suspicious files, the actual job detail pdf will always be sent to FortiGate. By default, for clean jobs, FortiSandbox will only send a template PDF.

Syntax

```
device-clean-pdf [-h|-l|-e|-d]
```

Option	Description
-h	Help information.
-e	Enable FSA to generate PDF report for clean rating jobs when requested by device.
-d	Disable FSA to generate PDF report for clean rating jobs when requested by device. A template PDF report is returned (default).
-l	Display the status of generating PDF report for clean rating jobs.

filesize-limit

Set the maximum single file size and the maximum child file size to scan.

The default limit for all file types is:

- File Size: 200M
- Uncompressed Size: 500M

Maximum file sizes:

Type	Compressed	Uncompressed
Device	512M	2048M
Ondemand /jsonrp	30720M	30720M
Netshare	10240M	10240M
Others	1024M	2048M

File size limitation for device is applicable to all devices, including both OFTP and Inline-Block mode.

Syntax

```
filesize-limit [-h|-l|-t[all|ondemand|netshare|jsonrpc|icap|device]-v[MB]-u[MB]]
```

Option	Description
`-h`	Help information.
`-l`	Display the file size limitation.
`-t[all|ondemand|sniffer|netshare|jsonrpc|icap|device|adapter]`	Set the input sources: `-v` Set the single file size limitation, in megabytes (0 - 1024). `-u` Set the total uncompressed file size limitation for an archive file, in megabytes (0 - 2048).

fortimail-expired

Enable/disable timeout check for FortiMail files. By default, FortiMail will hold mail for set period to wait for the verdict from FortiSandbox. Before FortiSandbox scans a file or URL that is sent from FortiMail, it will check if the verdict is still needed - FortiMail may have already released the email after timeout. If not, FortiSandbox will give the job an *Other* rating and a *skipped* status.

Syntax

```
fortimail-expired [-h|-e|-d|-l]
```

Option	Description
-h	Help information.
-e	Enable expired timeout for FortiMail files.
-d	Disable expired timeout for FortiMail files (default).
-l	Display the status of timeout feature for FortiMail files.

inline-block-timeout

Set the timeout value to reply to the request from FortiOS.

Syntax

```
inline-block-timeout [-a|-h|-l|-r|-s]
```

Option	Description
-a<skip/scan>	Set the action to take for the submitted file. If action is: • Skip (default): The file will be skipped. • Scan: The file will be sent to VM Scan.
-h	Help information.
-l	Display the current settings.
-r	Remove the settings and default values will be used.
-s[value]	Set timeout value in seconds (default = 50, range is 20 to 50).

paix-ioc

This command allows users to enable or disable enriched PAIX IOCs. When enabled, additional indicators may appear in the job details. For performance reasons, this feature is disabled by default.

An active PAIX contract is required to use this feature.

Syntax

```
paix-ioc [-h|-l|-e|-d]
```

Option	Description
`-h`	Help information.
`-l`	Show the current setting.
`-e`	Enable PAIX enriched IOCs.
`-d`	Disable PAIX enriched IOCs. (default)

pending-jobs

This command allows users to view job queues statistics and purge them.

Syntax

```
pending-jobs show|purge source jobqueue filetype
```

Option	Description
`-h`	Help information.
`show / purge`	Show or purge the pending jobs.
`source`	One of: • `all` • `inline-block` • `ondemand` • `rpc` • `device` • `fgt` • `fml` • `fct` • `fwb` • `sniffer` • `adapter` • `netshare` • `url` • `urlrpc` • `urldev` • `urlfgt` • `urlfml` • `urlfct` • `urlfwb` • `urladapter` • `urlsniffer` - URLs embedded in email body that are detected by sniffer.

Option	Description
jobqueue	One of: • all - All job queues. • vm - Sandobxing job queue. • nonvm - non-Sandboxing job queue. • pre - Files pending to enter job queue.
filetype	One of: • all • exe • pdf • doc • flash • web • image • url • android • mac • user • other

prescan-config

Large files are typically archive files that contain multiple embedded files. Configure the maximum file size supported by FortiSandbox using the filesize-limit command.

In a cluster environment, use this command only in the primary node and the setting is synchronized to other nodes.

We recommend to only specifying one option each time.

Syntax

```
prescan-config [-h|-l|-c|-a|-b|-z|-n|-y|-e|-f|-u]
```

Option	Description
-h	Help information.
-l	Show prescan configuration settings.
-c	Set maximum number of child files to extract from archive file. (Default 1000 for VM model)
-a	Set size limit (<100M) of the archive file that will be scanned with the executable file in VM (default 5M)

Option	Description
	When scanning executable child files within a ZIP archive, the parent archive may also be required because the executable files can reference other files inside the archive. FortiSandbox can send the parent ZIP file to the VM together with the executable child file during dynamic analysis. For performance reasons, the default maximum size of the parent archive that can be sent to the VM is 5 MB. This value can be increased up to 100 MB if required. • This setting applies only to parent archive files sent to the VM together with executable child files. • For single files, the maximum size supported for dynamic (VM) analysis is 512 MB due to VM clone resource limitations. This limit is not configurable.
`-b`	Set large file (>512MB) unpack timeout in seconds (default = 600, max = 86400).
`-z`	Set large file (>512M) yara scan timeout in seconds (default = 60, max = 3600)
`-n`	Set regular file (<=512MB) unpack timeout in seconds (default = 15, max = 3600).
`-y`	Set regular file (<=512M) yara scan timeout in seconds (default = 30, max 3600)
`-e`	For text files, determine the file type using the file extension; if no extension is present, fall back to content-based detection (default).
`-f`	For text files, determine the file type strictly based on content.
`-u`	Unset all prescan settings, that is, set to default.

The unpack timeout and number of child files can be increased to improve threat detection. For more information, see *Enhancing Threat Detection* in the FortiSandbox Best Practices Guide.

processing-jobs

Use this command to display or purge the jobs in process. After canceling the jobs in processing, the job status is shown as *Canceled* in the job details.

Syntax

```
processing-jobs [show|cancel|-j<job_id>]
```

Option	Description
`show`	Show the number of jobs in process.
`cancel`	Cancel the processing jobs.

Option	Description
-j<job_id>	Show the details of a job by its job ID. You can use a comma to separate IDs. A maximum 64 jobs is allowed.

Examples:

To display all the jobs in process:

```
processing-jobs show
```

To cancel all the jobs in process:

```
processing-jobs cancel
```

To display one job:

```
processing-jobs show -j6565044453198669436
```

To cancel one job:

```
processing-jobs cancel -j6565044453198669436
```

sandboxing-adaptive

Turn adaptive scan on or off.

Not all FSA models support adaptive Scan, for more information, please refer to Scan Profile Advanced Tab | FortiSandbox 4.4.3 | Fortinet Document Library (a link to Adaptive Scan in Scan Profile section in Admin Guide)

Not all FortiSandbox models support Adaptive Scan. For more information, see *Adaptive Scan* in Scan Profile Advanced Tab of the Administration Guide.

Syntax

```
sandboxing-adaptive [-h|-l|-e|-d]
```

Option	Description
-h	Help information.
-e	Enable adaptive sandboxing scan.
-d	Disable adaptive sandboxing scan (default).
-l	Display the adaptive sandboxing scan status.

sandboxing-embeddedobj

Turn this option on or off to analyze embedded URLs, QR codes, and executable files contained within files.

By default, up to 3 embedded URLs and 3 embedded files are analyzed inside the VM for each submitted file. The maximum supported limits are 30 embedded URLs and 30 embedded files.

Syntax

```
sandboxing-embeddedobj [-h|-l|-t|-n]
```

Option	Description
`-h`	Help information.
`-l`	Display the settings
`-t`	Specify object type: `file | url | image | qr | ocr`.
`-n`	<0–30> When the type is file or URL, this setting defines the maximum number of embedded objects to scan in the VM. A value of 0 disables extraction. The default value is 3. When the type is image, QR code, or OCR, a value of 0 disables extraction, while any non-zero value enables extraction. The default value is 0. The configuration can be set or unset on a standalone or primary unit. In cluster mode, the setting is synchronized across all nodes.

sandboxing-parallel

Turn parallel scan on or off.

Syntax

```
sandboxing-parallel [-h|-l|-e|-d]
```

Option	Description
`-h`	Help information.
`-e`	Enable parallel sandboxing scan.
`-d`	Disable parallel sandboxing scan (default).
`-l`	Display the parallel sandboxing scan status.

sandboxing-pipeline

Pipeline Mode improves performance and accelerate the scan by reducing the time spent on VM instance starts and shutdowns. This allows jobs to be scanned in a VM instance one by one without shutting down the instance.

Syntax

```
sandboxing-pipeline [-h|-e|-d|-l]
```

Option	Description
-h	Help information.
-l	Display the status of sandboxing pipeline mode.
-e	Enable local sandboxing pipeline mode.
-m	Maximum number of jobs to be scanned in the pipeline, 50 by default.
-d	Disable local sandboxing pipeline mode (default).

sandboxing-prefilter

Allow user to turn FortiGuard prefiltering on or off for certain file types.

If a file type is associated with a guest VM image, it will be scanned if the file type enters the job queue as defined in the *Scan Profile* page. You can turn on FortiGuard prefiltering for a file type so that files of that type will be statically scanned first by an advanced analytic engine, and only suspicious files will be sandboxing scanned by the guest image. This can improve the system's scan performance, and all files will still go through an AV scan, a static scan, and community cloud query steps.

For the URL type, when FortiGuard prefiltering is enabled, only URLs whose web filtering rating is Unrated will be scanned inside associated guest VM image.

Syntax

```
sandboxing-prefilter [-h|-l|-e|-d] -t
     [dll|pdf|swf|js|htm|url|office|trustvendor|trustdomain|archive|trustfndr]
```

Option	Description
-h	Help information.
-e	Enable sandboxing prefilter. • -t [dll|pdf|swf|js|htm|url|office|trustvendor|trustdomain|archive|trustfndr]:

Option	Description
	Enable sandboxing prefilter for specific types.
`-d`	Disable sandboxing prefilter (default). • `-t [dll|pdf|swf|js|htm|url|office|trustvendor|trustdomain|archive|trustfndr]`: Disable sandboxing prefilter for specific types.
`-l`	Display the status of sandboxing prefilter.
`-t`	Enable/disable sandboxing prefilter for specific file types: `archive`, `dll`, `pdf`, `swf`, `js`, `htm`, `url`, `office`, `trustvendor`, `trustdomain`,`trustfndr`. `archive` and `trustdomain` are enabled by default. Other prefilters are disabled by default. When `trustvendor` is selected, executable files from a small internal list of trusted vendors will skip the sandboxing scan step. When `trustdomain` is selected, files downloaded from a small internal list of trusted domains will skip the sandboxing scan step. When `trustfndr` is selected, files rated by FortiNDR as clean or malicious will skip the sandboxing VM scan step.

sandboxing-ratio

Turn VM scan ratio on or off.

Syntax

```
sandboxing-ratio [-h|-s|-r|-l]
```

Option	Description
`-h`	Help information.
`-s`	Set customized ratio (low bound) of jobs to be scanned in sandboxing, from 0 to 100. 0 means no customized setting on the ratio (default). 100 means all jobs are scanned in sandboxing.
`-r`	Reset local VM scan ratio statistics.
`-l`	Display the customized sandboxing ratio.

sandboxing-rse

Turn rating service endpoint API on or off. When off, FortiSandbox uses local rating source. When on, FortiSandbox uses it as the rating source only when the results returned by the rating service are different from the results from local rating.

Syntax

```
sandboxing-rse [-h|-l|-e|-d]
```

Option	Description
-h	Help information.
-e	Enable rating service endpoint.
-d	Disable rating service endpoint (default).
-l	Display the status of rating service endpoint.

scan-perf

Retrieve system scan performance statistics, including both static and dynamic scans, for up to the past 28 days.

Syntax

```
scan-perf [-h|-m|-o|-d]
```

Option	Description
-h	Help information
-m<mins>	Scan performance for the last <mins> minutes (max 40320)
-o<hours>	Scan performance for the last <hours> hours (max 672)
-d<days>	Scan performance for the last <days> days (max 28)

url-deep-check

Use this command to view, configure, and control advanced URL inspection features that analyze URLs for potential security threats, including payload inspection, RTAP integration, and recursive URL analysis.

Syntax

```
Usage: url-deep-check [-h|-l|-e|-d|-u] [-f|-a|-p|-r]
```

Option	Description	
-h	Display help information.	
-l	Show current URL deep check configuration.	
-e |-d	Enable/Disable specific URL deep check features.	
	-f	Payload inspection (Enabled by default).
	-a	RTAP checks for all URLs (RTAP subscription required).
	-p	RTAP checks for URLs during dynamic scans (Enabled by default, RTAP subscription required).
	-r	Recursive URL checks (Up to 30 URLs).
-u	Reset URL deep check configuration to default.	

url-recheck

Enable/disable trusting previous scan results in Fortimail URL scan.

Syntax

```
url-recheck [-h|-e|-d|-l]
```

Option	Description
-h	Help information.
-e	Enable Fortimail URL scan without trusting previous scan results
-d	Disable Fortimail URL scan by trusting previous scan results (default).
-l	Display the status of this setting.

System commands

The following system commands are available:

Command	Description
`backup-sysconf`	Upload system configuration backup to remote server.
`change-password`	Local users can use this CLI to change passwords.
`cleandb`	Clean up the internal database and job information. This command erases all stored data and reboots the device. This command only works on devices that are in standalone mode.
`cm-status`	List the status of units joining the Global Threat Information Network.
`config-reset`	Reset the FortiSandbox configuration to factory default settings. Job data is kept. For installed VM images, their clone numbers and *Scan Profile* settings are set back to default.
`confirm-id`	Set confirm ID for Microsoft Windows or Office activation.
`device-authorization`	Configure new client device authorization .
`device-ssl`	Enable/disable TLS 1.3 protocol and specific SSL CBC Suites protocol.
`factory-reset`	Reset the FortiSandbox configuration to factory default settings. All data is deleted. For installed VM images, only Default VMs are kept and their clone number and *Scan Profile* settings are set back to default.
`fsck-storage`	Check the file system on the hard disk and repair it if it's not clean. System reboots immediately.
`fw-upgrade`	Upgrade or re-install the FortiSandbox firmware via Secure Copy (SCP) or File Transfer Protocol (FTP) server.
`lightning-mode`	Enable or disable Lightning Mode.
`log-dropped`	Enable/disable the log file drop event.
`log-purge`	Delete all system logs.
`ps-status`	Use this command to display power supply status. At this time, this command is only supported on FSA 2000E, 3000E, 3000F, 3000G and 1500G models.
`reboot`	Reboot the FortiSandbox. All sessions will be terminated. The unit goes offline and there is a delay while it restarts.
`remote-auth-timeout`	Set the timeout for remote authentication.
`rename-admin`	Administrators with the *Super Admin* profile can use this command to rename other administrators.
`reset-sandbox-engine`	Reset the tracer/rating engine back to firmware default.

Command	Description
reset-scan-profile	Reset the scan flow settings to firmware default values.
reset-widgets	Reset the GUI widgets.
resize-hd	After the user changes the virtual hard disk size on the hypervisor, execute this command to make the firmware recognize this change. This command is available only on VM models.
restore-sysconf	Restore system configuration from remote server. For details, see restore-sysconf on page 51.
sandbox-engines	Display FortiSandbox FortiGuard component versions including the Tracer Engine, Rating Engine, Traffic Sniffer, Botnet Signature Database, IPS Signature Database, and Android engine versions.
set-cfg-backup-key	Set your own passphrase that openSSL uses to encrypt or decrypt a configuration backup file.
set-maintainer	Enable/disable the maintainer account.
set-tcp-timestamp-response	Set tcp timestamp reponse.
set-tlsver	Set the allowed TLS version for HTTPS service.
shutdown	Shutdown the FortiSandbox.
status	Display the FortiSandbox firmware version, serial number, system time, disk usage, disk inode usage, image status check, Microsoft Windows VM status, VM network access configuration and RAID information. The CLI will also display database status when it is not ready.
system-admin	Create/Delete an Administrator.
upload-settings	Configure data upload settings to community cloud.
set-dare-encryption	Enable data-at-rest encryption, or list the current configuration state.
usg-license	Convert the unit to be USG licensed.

backup-sysconf

Upload system configuration backup to remote server.

Syntax

```
backup-sysconf [-s|-t|-u|-f]
```

Option	Description
-s<server IP>	Remote server IP address.
-t[scp|tftp]	Upload protocol.
-u<username>	Username for server authentication.
-f<fpath>	Upload path including file name.

Example:

```
backup-sysconf -s10.0.0.5 -ttftp -utestuser -ffsa.conf
```

change-password

Local users can use this CLI to change passwords.

Sytnax

```
change-password [-h|-c]
```

Option	Description
-h	Help information.
-c	Change current user password.

Example

```
> change-password -c
Enter current password:
Validating...
Enter new password: ********
Confirm new password: ********
Password changed successfully.
```

cleandb

Clean up the internal database and job information. This command erases all stored data and reboots the device.

This command only works on devices that are in standalone mode.

Sytnax

```
cleandb
```

cm-status

List the status of units joining the Global Threat Information Network.

Syntax

```
cm-status [-h|-l|-a]
```

`-h`	Help information.
`-l`	List the status of active Central Malware units.
`-a`	List the status of all Central Malware units.

config-reset

Reset the FortiSandbox configuration to factory default settings. Job data is kept.

For installed VM images, their clone numbers and *Scan Profile* settings are set back to default.

Sytnax

```
config-reset
```

confirm-id

Validate a Microsoft Windows or Office key after contacting Microsoft customer support. For more details, please contact Fortinet Customer Support.

Syntax

```
confirm-id [-a|-d|-l]
```

Option	Description
-a	Add a confirmation ID: -k License key or username from account information. -c Conformation ID. -n Name of VM.
-d	Delete a confirmation ID: -k License key or username from account information.
-l	List all confirmation IDs.

Example

The following sytax will add a confirmation ID for VM WIN7X64VM:

```
confirm-id -a -kSGWGG-J668H-X2VMG-6FBRW-XXXXX -c50518649351137250155400508016393350046692078366 2 -
      nWIN7X64VM
```

device-authorization

Users can decide to either manually or automatically authorize a new client device.

Syntax

```
device-authorization [-h|-a|-m|-e|-o|-f|-l]
```

Option	Description
-h	Help information.
-a	When a new device other than FortiClient registers, FortiSandbox will authorize it automatically.
-m	When a new device other than FortiClient registers, user has to authorize it manually from WebUI.
-e	Authorize all existing devices if they are not.
-o	When a new FortiClient registers, it inherits authorization status from managing EMS or FGT, or user has to change it manually from WebUI.
-f	When a new FortiClient registers, FortiSandbox will authorize it automatically.
-l	Display the status of device and FortiClient authorization. Default: manually.

Example

```
device-authorization -a -f
```

- Device authorization is automatic.
- FortiSandbox will authorize FortiClient automatically.

device-ssl

Enable/disable TLS 1.3 protocol and specific SSL CBC Suites protocol.

Syntax

```
device-ssl [-h|-l|-g|-f|-j|-k]
```

Option	Description
-h	Help information.
-l	Display current support status for TLS 1.3 and weak cert/algorithm.
-g	Enable TLS 1.3 for devices (default).
-f	Disable TLS 1.3 (max 1.2) for devices.
-k	Allow weak cipher suite and cert.
-j	Do not allow weak cipher suite and cert (default).

factory-reset

Reset the FortiSandbox configuration to factory default settings. All data is deleted.

For installed VM images, only Default VMs are kept and their clone number and *Scan Profile* settings are set back to default.

Syntax

```
factory-reset
```

format-storage

Use this command to remove sensitive data from the hard disk without delating the default Windows VMs. This saves time re-installing the VM packages.

After the command is finished, the unit will be in factory reset status, meaning all the data will be deleted and all the configurations are reset. However, the activated default VMs are kept without losing their activated status.

Executing the command will take several hours to complete. Do not power off or reboot the unit during execution. After the command is finished, all settings are reverted back to the default values, including network settings, so a console connection is recommended.

Before executing the command, ensure the console is connected to set the password and IP.
This command is not available on VM appliances, or lower-end hardware appliances 500F and 500G.
This command is only supported in Standalone mode.

Syntax

```
format-storage [-k]
```

Option	Description
-k	A base64-encoded passphrase can be used to encrypt the HDDs. The decoded passphrase must be 8–32 characters long and contain at least one uppercase letter, one lowercase letter, one digit, and one special character (e.g., !, @, #, $). This option is exclusive to FSA 3000G hardware appliances.

Example

```
format-storage
         This command will zero fill and format the storage disk! All data will be lost!
Configurations will be reset to factory default! Please do not interrupt or turn off power!
Do you want to continue? (y/n)

Confirm with answer ‘y’, another confirm shows up:
Dangerous operation! System will reboot immediately. Storage disk will be formatted.
Do you want to continue? (y/n)
```

FAQs

Question	Answer
Which platforms support this feature?	Currently, only 3000G supports this feature.
Where is the passphrase stored and how secure is this storage?	It is stored on the RAID controller.
What is the scope of encryption?	Full disk encryption.
What algorithms or technologies are used?	Self-Encrypting Drive (SED) with TCG Encryption.
What controller models are in use?	MegaRAID 9560-8i.
Does the RAID controller verify if it's plugged into the same FSA hardware?	Yes.

fsck-storage

Check the file system on the hard disk and repair it if it's not clean. System reboots immediately.

Syntax

```
fsck-storage
```

fw-upgrade

Upgrade or re-install the FortiSandbox firmware or VM or FortiGuard engines via SCP, FTP, or HTTPS server. Before running this option, download the firmware or VM or FortiGuard engines file to a server that supports file copy via FTP/SCP/HTTPS.

For firmware installation, the system will reboot after the firmware is downloaded and installed.

This CLI supports proxy server by `-x` option.

Syntax

```
fw-upgrade [-h|-b|-v|-e|-x]
```

Option	Description
`-h`	Help information.

Option	Description
-b	Download an image file from this server and upgrade the firmware.
-v	Download a VM image file from this server and install.
-e	Download a system rating/tracer engine from this server and install.

Option	Description
-t<ftp|https|scp>	The protocol type, FTP/HTTPS/SCP. The default is scp.
-s<SCP/FTP/HTTPS server IP address>	Download an image file from this server IP address.
-u<user name>	The user name for authentication.
-f<full path of filename>	The full path for the image file.
-x[t|s|p|u|w]	Proxy server configuration.

Option	Description
-xt[http|socks4|socks5]	Proxy server type.
-xs	Proxy server IP or FQDN name.
-xp	Proxy server port.
-xu	Proxy server authentication username.
-xw	Proxy server authentication password.

Example

Download a VM image file from the server and install:

```
fw-upgrade -v -tscp -s172.17.58.136 -utest -f/home/test/WIN7X64VM.pkg
```

Install using the proxy server:

1. Install the firmware image:
   ```
   fw-upgrade -b -tscp -s10.10.10.8 -ufsauser -f/home/fsa-test/vm2364.deb -ppassword -xthttp -
   xs10.10.9.8 -xp808 -xuproxyuser1 -xwproxypassword
   ```
2. Install the VM in FortiSandbox:
   ```
   fw-upgrade -v -thttps -sfsavm.fortinet.net -f/images/v4.00/AndroidVM_2.pkg -xthttp -xs10.10.9.8
   -xp808 -xuproxyuser1 -xwproxypassword
   ```
3. Install the FortiGuard package:
   ```
   fw-upgrade -e -tscp -s10.10.10.8 -ufsauser -f/home/fsa-test/t440.pkg -ppassword -xtsocks5 -
   xs10.10.9.8 -xp1080 -xuproxyuser1 -xwproxypassword
   ```

lightning-mode

Enable or disable Lightning Mode.

Syntax

```
lightning-mode [-h|-l|-e|-d]
```

Option	Description
-h	Help information.
-e	Enable Lightning mode.
-d	Disable Lightning mode (default).
-l	Display the status of Lightning mode.

lite-mode

Enable or Disable the Lite Mode.

Syntax

```
lite-mode [-h|-l|-e|-d]
```

Option	Description
-h	Help information.
-e	Enable Lite mode.
-d	Disable Lite mode (default).
-l	Display the status of Lite mode.

log-dropped

Enable or disable the log file drop event.

Syntax

```
log-dropped [-h|-l|-e|-d]
```

Option	Description
-h	Help information.
-l	Show the current configuration.
-e	Enable log dropped file.
-d	Disable log dropped file (default).

log-purge

Delete all system logs.

Syntax

```
log-purge
```

ps-status

Use this command to display power supply status. At this time, this command is only supported on FSA 2000E, 3000E, 3000F, 3000G and 1500G models.

Syntax

```
ps-status
```

reboot

Reboot the FortiSandbox. All sessions will be terminated. The unit goes offline and there is a delay while it restarts.

Sytnax

```
reboot
```

remote-auth-timeout

Set Radius or LDAP authentication timeout value.

Syntax

```
remote-auth-timeout [-h|-s|-u|-l]
```

Option	Description
-h	Help information.
-s	Set the timeout value, in seconds (10 - 180, default = 10).
-u	Unset the timeout value.
-l	Display the timeout value.

rename-admin

Administrators with the *Super Admin* profile can use this command to rename other administrators.

This command is available only on standalone and primary nodes.

The default administrator (*admin*) cannot be deleted with the GUI. To delete the admin:

1. Use rename-admin to rename the admin.
2. Delete the renamed admin with the GUI.

Syntax

```
rename-admin [-h| -u | -n]
```

Option	Description
-h	Help information.
-u<username>	Username should be an existing administrator.
-n<new-username>	● Username should follow username format guideline. ● New-username cannot be admin. ● New-username should not be same as an existing administrator.

Before renaming the default admin:

- Backup the admin to ensure you can restore it if you change your mind.
- Ensure the administrator is not logged in.

For information about default administrators, see Administrators in the *FortiSandbox Administration Guide*.

After renaming the default admin:

- You cannot use the GUI to recreate the default admin.
- You can create *admin* in maintainer mode.

Example

```
rename-admin –uadmin –nnewadmin
WARNING: You are going to rename an Administrator name. Please make sure you have closed all
      administrative access sessions of this user, including web GUI, SSH/Telnet etc. Do you want to
      continue? (y/n)y
```

reset-sandbox-engine

Reset tracer and rating engines back to firmware default.

Syntax

```
reset-sandbox-engine [-h|-t|-r|-p|-b]
```

Option	Description
-h	Help information.
-t	Reset tracer engine to firmware default.
-r	Reset rating engine to firmware default.
-p	Reset AI Engine and Model to base.
-b	Reset Tracer, Rating and AI Engines/Models to base.

reset-scan-profile

Reset the scan flow settings to firmware default values. These settings are also displayed in the GUI under *Scan Profile page > Pre-filter > VM Association > Advanced tab.*. VM clone numbers and their file extension association are not changed.

This command is only supported on standalone or Primary units in a cluster.
-v option only available on standalone unit.

Syntax

```
reset-scan-profile [-h|-p|-v|-a]
```

Option	Description
-h	Help information.
-p	Reset Pre-Filter in Scan Profile.
-v	Reset VM Association in Scan Profile.
-a	Reset Advanced in Scan Profile.

reset-widgets

Reset the GUI widgets.

Sytnax

```
reset-widgets
```

resize-hd

Execute this command to force the firmware to recognize changes to the virtual hard disk size on the hypervisor. The unit will be reboot after entering y for the confirmation question.

This command is only available for FSAVM00 models.

Syntax

```
resize-hd
```

restore-sysconf

Restore system configuration from a configuration backup in a remote server.

Syntax

```
restore-sysconf [-s|-t|-u|-f|-o]
```

Option	Description
-s<server IP>	Remote server IP address.
-t<scp|ftp|tftp>	Download protocol.
-u<username>	Username for server authentication.
-f<fpath>	Configuration backup full path.
-o	Restore user authentication.

Example

```
restore-sysconf -s10.0.0.5 -tscp -utestuser -ffsa/backup/FSA_b0261.conf -o
```

sandbox-engines

Display FortiSandbox FortiGuard component versions including the Tracer Engine, Rating Engine, AI Engine and Model, Traffic Sniffer, Botnet Signature Database, IPS Signature Database, and Android engine versions.

Syntax

```
sandbox-engines
```

set-cfg-backup-key

Set your own passphrase that openSSL uses to convert into an encryption/decryption key to encrypt or decrypt a configuration backup file.

Syntax

```
set-cfg-backup-key [-h|-s|-r]
```

Option	Description
-h	Help information.
-s	Set configuration backup encryption key.
-r	Reset configuration backup encryption key to default.

set-dare-encryption

Enable data-at-rest encryption, or list the current configuration state.

When encryption is enabled, you are prompted for a passphrase between 8 and 64 characters, which is used to generate the encryption key. You must enter this passphrase at the console every time the FortiSandbox boots. Do not lose this passphrase, if you do, the FortiSandbox will not be able to boot and will become unusable.

- For VMs: you must restore a snapshot or reinstall.
- For hardware appliances: an RMA is required.

- This configuration currently encrypts only user configuration data and job data, including pending and finished jobs.
- DARE mode cannot be enabled while FortiSandbox is part of a cluster; however, the unit may join a cluster after DARE is enabled.
- DARE settings are not synchronized across cluster members.
- File sizes will increase by 8 KB to 12 KB after encryption.
- The only supported method to disable DARE is to run a CLI `factory-reset`.
- This CLI is not available on virtual cloud and E models.

Syntax

```
set-dare-encryption [-h|-l|-e]
```

Option	Description
-h	Help information.
-l	List data-at-rest encryption status.
-e	Enable data-at-rest encryption.

Examples

Example:

```
FSASN> set-dare-encryption -h

Usage: set-dare-encryption [-h|-l|-e]

        -h Help information

        -l List data-at-rest encryption status

        -e Enable data-at-rest encryption

FSASN >

FSASN > set-dare-encryption -l

Data-at-rest is not encrypted

FSASN >
```

Example:

```
FSASN > set-dare-encryption -e

Data-at-rest encryption requires a passphrase. It will need to be entered at
the Console each time the device is powered on.

WARNING:  Do not lose this passphrase as the device will not function
correctly without entering the exact passphrase.  Data is not recoverable
without the passphrase.

The system will be rebooted after entering the passphrase twice.

Do you want to continue? (y/n)y

Enter DARE passphrase: ********

Enter DARE passphrase: ********

Finished creating dare encryption for config data.

FSASN > set-dare-encryption -l

Data-at-rest encryption is active

FSASN >
```

set-maintainer

The maintainer account is used to reset users' passwords.

Syntax

```
set-maintainer [-h|-l|-d|-e]
```

Option	Description
-h	Help information.
-l	Show current setting.
-d	Disable maintainer account.
-e	Enable maintainer account (default).

set-tcp-timestamp-response

FortiSandbox responds with a TCP timestamp which can be used to approximate the remote hosts uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

Syntax

```
set-tcp-timestamp-response [-e|-d|-l|-h]
```

Option	Description
-h	Help information.
-l	Show current TCP timestamp response setting.
-e	Enable TCP timestamp response (default).
-d	Disable TCP timestamp response.

set-tlsver

Set the supported TLS version for HTTPS service.

Syntax

```
set-tlsver [-h|-l|-r|-e]
```

Option	Description
`-h`	Help information.
`-l`	Show the current TLS versions.
`-r`	Reset to default versions (TLSv1.2 and TLSv1.3 are supported).
`-e[2|3]`	Set the supported TLS versions: `2` is for TLS 1.2 and `3` is for TLS 1.3 respectively. Separate versions with '|'. For example, `e2|3` will enable both TLS 1.2 and 1.3 TLSv1.0 and TLSv1.1 are not supported.

shutdown

Shutdown the FortiSandbox.

Syntax

```
shutdown
```

status

Display the FortiSandbox firmware version, serial number, system time, disk usage, disk inode usage, image status check, Microsoft Windows VM status, VM network access configuration and RAID information. The CLI will also display database status when it is not ready.

Syntax

```
status
```

system-admin

Create or delete an administrator.

Syntax

```
system-admin [-h|-c|-d]
```

- Only administrators with the *Super Admin* profile have permission to use this command.
- This command cannot be used to create or delete the default *admin* user.
- This command is available only on standalone and primary nodes.
- This command is not available for public cloud platforms (AWS, AZURE, GCP, OCI, PaaS) FSA.
- All parameters must not contain spaces.
- During command-line execution, the system will prompt for Password and Confirm Password inputs, which are mandatory for setting or confirming the system administrator's password. The passwords entered will be hidden for security reasons, ensuring confidentiality and consistency.
- Unlike the GUI, this command does not have the *Comments* and *Default On-Demand Submit settings* options.
- Two-factor Authentication is limited to FortiSandbox appliances and FSA-VM0T, contingent upon the purchase of the FortiToken Cloud service.

Option	Description
`-c`	Create an Administrator account. **Option** / **Description** `-u` Administrator account name. `-e` Email address `-o` Phone number `-f` [super-admin|read-only|device|netshare|<user defined profile>] Administrator account profile `-t` [local|ldap|radius|ldap_wildcard|radius_wildcard] Administrator account type `-w` [FTM|SMS|EMAIL] Two-factor authentication method `-l` [en-us|ja|fr] Language preference `-ld` LDAP server `-lr` RADIUS server `-t4` Trusted IPv4 hosts, separated by ; `-t6` Trusted IPv4 hosts, separated by ; `-gd` Device group `-gn` Netshare group.
`-d`	Delete an Administrator account `-u` Administrator account name.
`-h`	Help information

Examples

Create a local Super Admin user:

```
system-admin -c -utest_user -eexample_email@fortinet.com -o+10123456789 -fsuper-admin -tlocal -
len-us -t4192.168.1.0/255.255.255.0;192.168.2.0/255.255.255.0; -
t6fd13:6918:e38c:edd5::1/64;fd13:6919:e38c:edd5::1/64;

Password:

Confirm Password:
```

Delete an existing user:

```
system-admin -d -utest_user
```

upload-license

Download firmware license file from a remote server and install it.

This command is only available for VM appliances.

FortiSandbox will reboot immediately after the license is uploaded.

Syntax

```
upload-license [-h|-s|-t|-u|-f]
```

Option	Description
-h	Help information.
-s<server ip>	Download a license file from this server IP address.
-t[scp|ftp]	The download protocol type. The default is scp.
-u<user name>	The user name for server authentication.
-f<license filename>	The full path for the license file.

Example:

```
upload-license -s10.59.2.18 -tscp -uadmin -fworkspace/FSAVM.lic
```

upload-settings

Configure data upload settings to community cloud.

Syntax

```
upload-settings [-h|-e|-d|-t|-l]
```

Option	Description
`-h`	Help information.
`-e`	Enable the specified upload setting.
`-d`	Disable the specified upload setting.
`-t[uploadcloud|submiturl|uploadstats]`	Set the type of upload setting: **Options** / **Description** `uploadcloud` — Upload malicious and suspicious file information to Sandbox Community Cloud. Default is enabled. `submiturl` — Submit suspicious URL to Fortinet WebFilter service. Default is disabled. `uploadstats` — Upload statistics data to FortiGuard service. Default is disabled.
`-l`	Display the status of the upload settings

Example

To enable upload statistics to FortiGuard services:

```
upload-settings -tuploadstats -e
```

usg-license

Convert the unit to be USG licensed. When a USG license is applied, only FortiGuard Distribution Network (FDN) servers in the United States can be used.

syntax

```
usg-license [-h|-l|-s|-r]
```

Option	Description
`-h`	Help information.
`-l`	List the USG license status.
`-s<USG-license-string>`	Set this unit to be USG licensed.
`-r<Regular-license-string>`	Revert the unit back to a regular license.

Virtual Machine (VM)

The following VM commands are available:

vm-customized	Install a customized VM and download a customized VM image from FortiSandbox.
vm-internet	The command is used to setup the gateway and DNS if allow virtual machines to access external network through outgoing port3.
vm-license	Use this command to list embedded Windows Product key and contract information.
vm-reset	Use this command to delete and then reinstall a Virtual Machine. The VM status will be *Installed*.
vm-status	Show VM system status and license. If there is an issue with a VM, an error message displays information to help troubleshoot the problem.

vm-customized

Install a customized VM and download a customized VM image from FortiSandbox.

Syntax

```
vm-customized <option> ... <option>
```

Option	Description
`-h (or --help)`	Help information.
`-c[n|l|f|d|u]`	Operation command.

Option	
`n`	Install a new customized VM.
`l`	List installed customized VM.
`f`	Upload a meta file for a customized VM.
`d`	Display a meta file for a customized VM.
`u`	Upload a VDI file to a remote server. Supported protocols include TFTP, FTP, and SCP.

Option	Description
-t<ftp|scp|tftp>	The protocol type, FTP, SCP (default) or tftp.
-s<server IP>	Download the image file from this FTP or SCP server IP address.
-u<user name>	User name for authentication.
-f<full path of filename>	Full path for the image file or meta file.
-d<hardware/machine ID>	Original hardware ID or machine ID.
-k<MD5 checksum>	MD5 checksum for the uploaded file.
-v[o|n|c|m]	Set the base information for VM image

Option	Description
o<OS type>	Windows10, or Windows10_64,Windows11_64, Linux, Linux_64.
n<VM name>	Name of the VM.
c<CPU>	CPU number, 1-4
m<Memory>	Memory size in MB, 1024-4096

-r <VM name>	Replace the VM if it already exists.
-m <VM meta file name>	Name of the VM meta file.

Example:

```
vm-customized -cn -tftp -s10.0.1.10 –uuser1 -p123456 -f/vm/Win10Entx64.vdi -voWindows10_64 -
      vnWin10Entx64 -kd3e1953cd39268e783854c7ba4897761 -r -vm2048 -vc2
```

vm-internet

Syntax

```
vm-internet [options]
```

Option	Description
-h (or --help)	Help information.
-l	Display the current configuration.
-s	Set port3 configurations used for URL content check and VM instance's Internet access.

Option	Description
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>-g<gateway IP></td><td>Next hop gateway IP address.</td></tr><tr><td>-d<DNS server IP></td><td>DNS server IP address.</td></tr></table>
-u	Unset port3 configurations used for URL content check and VM instance's Internet access.

vm-license

Use this command to list embedded Windows Product key and contract information.

Syntax

```
vm-license [-h|-l]
```

Option	Description
-h (or --help)	Help information.
-l	Displays a list of the Windows Product key information and contract information. For example, Antivirus, Web Filtering, Mail Transfer Agent Service, etc)

vm-reset

Use this command to delete and then reinstall a Virtual Machine. The VM status will be *Installed*. If the machine is a customized VM, the command will remove the activated VM and the status in the GUI will be *Installed*. When only customized VMs exist in FSA AWS and Azure, the command will delete/terminate all the clones and their resources. In the GUI, status will be kept.

Syntax

```
vm-reset [-n<vm name>]
```

Option	Description
-n<vm name>	Resets one virtual machine at a time

If you do not specify a VM name all VMs will be reset.

vm-status

Show VM system status and license. If there is an issue with a VM, an error message displays information to help troubleshoot the problem.

Syntax

```
vm-status
```

Utility commands

The following utilities are available.

Command	Description
ping	Test network connectivity to another network host:
tcpdump	Examine local network traffic
traceroute	Examine the route taken to another network host:

ping

Test network connectivity to another network host:

Syntax

```
ping <IP address> [-c]
```

Option	Description
IP address	Network IP address.
-c count	The count for sending packets.
-c0 continuous ping	Continuous ping.

Example:

```
ping 172.10.0.4 -c4
```

tcpdump

Examine the route taken to another network host.

Syntax

```
tcpdump [-c count| -i interface |expression]
```

Option	Description
`-c count`	The count for capturing packets.
`-i interface`	The interface name, (for example `port1`).
`expression`	Selects which packets will be dumped. If no expression is provided, all packets on the net will be dumped. Otherwise, only packets for which expression is `true` will be dumped.

Example:

```
tcpdump -c 3 -i port1
```

traceroute

Examine the route taken to another network host.

Syntax

```
traceroute <host>
```

Example:

```
traceroute 172.10.0.1
```

Change log

Date	Change Description
2025-06-08	Initial release of v5.2.0

www.fortinet.com