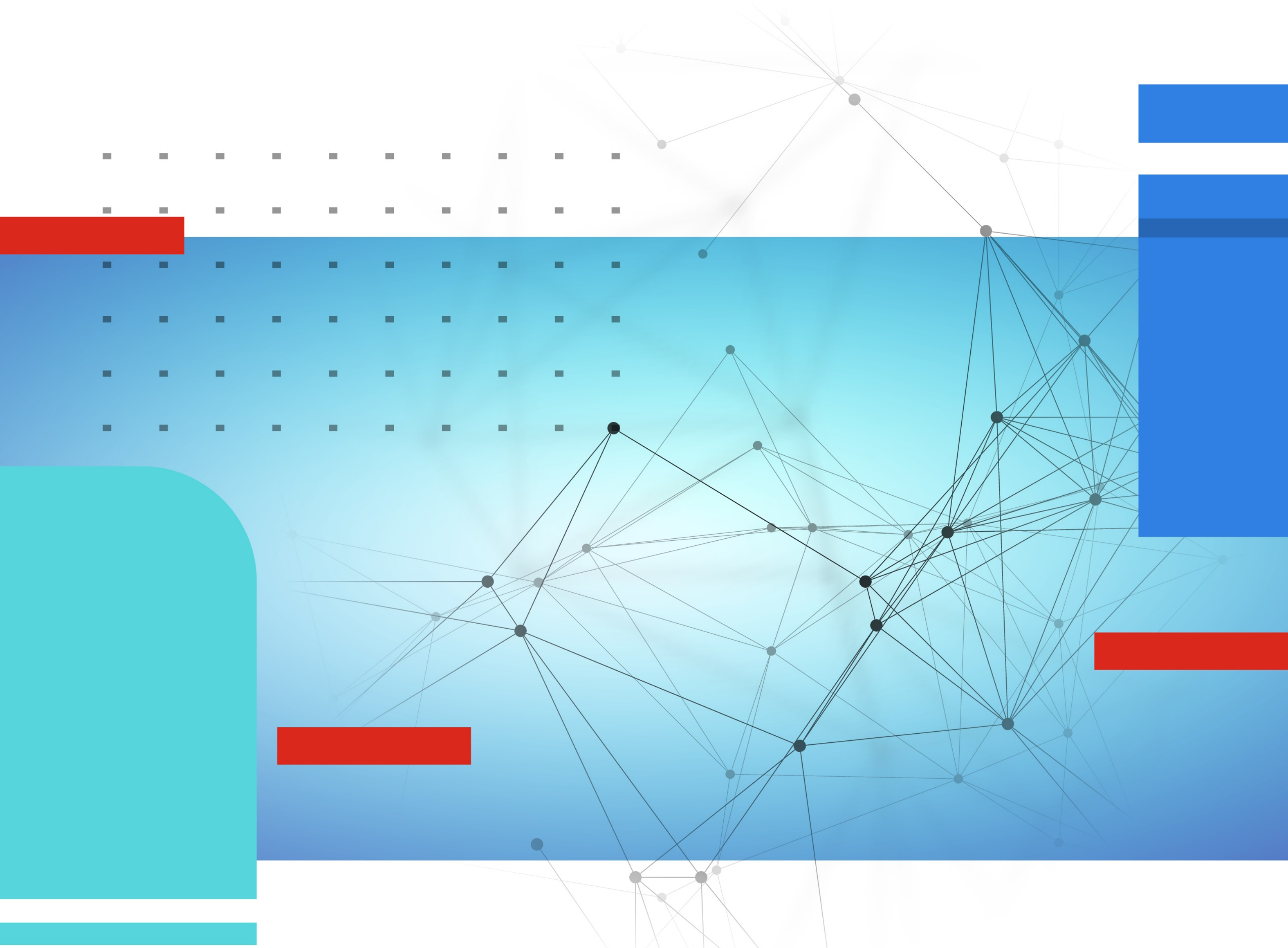
CLI Reference Guide

FortiSandbox 5.0.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 25, 2024
FortiSandbox 5.0.1 CLI Reference Guide
34-501-1102546-20250225

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
port3-speed	auto speed {full|half}	Set port3 speed and duplex settings. The option port3-speed is not supported on	port3-speed 1000 full, port3-speed auto

Attribute	Value	Description	Example
		FSA_VM.	
`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, 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.
`tac-report`	A collection of config, diagnose, 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.

Option	Description
`-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] [device_serial_number]
```

Option	Description
`adapter_bcc`	Daemon for BCC.
`adapter_icap`	Daemon for Internet Content Adaptation Protocol (ICAP).
`adapter_mta_list`	Pending emails for MTA Sending.
`adapter_mta_relay`	Daemon for MTA relay.
`anti-phishing`	Real-time Zero-Day Anti-Phishing Service.
`device`	OFTP daemon for FortiGate, FortiMail, and FortiClient devices.
`device_serial_number`	The device serial number.
`inline-block`	Inline block for FortiGate.
`netshare`	Network share daemon.

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.
`-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
```

tac-report

A collection of config, diagnose, system, and utility commands for monitoring and troubleshooting purposes.

Syntax

```
tac-report
Tac-report -l
```

Sample output

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

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 on page 17

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 Internet access 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
`fortiguard_upload`	Test statistics data submission to fortiguard service status

Option	Description
`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 19	Configure the unit as a HA-Cluster primary unit.
hc-settings on page 19	Configure the unit as a HA-Cluster mode unit.
hc-status on page 21	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 21	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|-u|-s|-l|-r]
```

Option	Description
`-h (or --help)`	Help information.
`-u`	Turn off file scan on primary unit.
`-s<10-100>`	Turn on file scan on the primary unit with 10% to 100% processing capacity (default = 50).
`-l`	Display the file scan status on primary unit.
`-r<serial number>`	Remove the worker unit from the HA-Cluster by its serial number.

hc-settings

Configure the unit as a HA-Cluster mode unit.

syntax

```
hc-settings [-h|-l|-sc|-t|-n|-c|-p|-i|-si|-a|-se|-sd]
```

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-h (or --help)</code></td><td>Help information.</td></tr>
<tr><td><code>-l</code></td><td>List the Cluster configuration.</td></tr>
<tr><td><code>-sc</code></td><td>Set this unit to be a HA-Cluster mode unit.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-t&lt;N|M|P|R&gt;</code></td><td>Set this unit to be a HA-Cluster mode unit.
<table>
<tr><td><code>N</code></td><td>N/A.</td></tr>
<tr><td><code>M</code></td><td>Primary unit.</td></tr>
<tr><td><code>P</code></td><td>Secondary unit.</td></tr>
<tr><td><code>R</code></td><td>Worker unit.</td></tr>
</table></td></tr>
<tr><td><code>-n&lt;name string&gt;</code></td><td>Set alias name for this unit.</td></tr>
<tr><td><code>-c&lt;HA-CLUSTER name&gt;</code></td><td>Set the HA-Cluster name for primary unit.</td></tr>
<tr><td><code>-p&lt;authentication code&gt;</code></td><td>Set the authentication code for primary unit.</td></tr>
<tr><td><code>-i&lt;interface&gt;</code></td><td>Set interface used for cluster internal communication.</td></tr>
</table></td></tr>
<tr><td><code>-si</code></td><td>Set the fail-over IPs for this cluster for primary unit.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-i&lt;interface&gt;</code></td><td>Specify the interface for external communication</td></tr>
<tr><td><code>-a&lt;IP/netmask&gt;</code></td><td>Specify the IP address and netmask for external communication. This IP address is applied as the alias IP of the specified interface. It must be in the same subnet as the unit IP subnet of the specified interface.</td></tr>
</table></td></tr>
<tr><td><code>-se</code></td><td>Enable traffic encryption between HA cluster members.</td></tr>
<tr><td><code>-sd</code></td><td>Disable traffic encryption between HA cluster members.</td></tr>
</table>

Example

```
hc-settings -sc -tM -nPrimay -cClusterTest -p1111 -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:

anti-phishing on page 23	Use this command to check URLs using the Real-time Zero-Day Anti-Phishing service. This feature is more sensitive for detecting phishing links compared with previous versions of URL detection.
device-clean-pdf on page 23	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 24	Set the maximum single file size and the maximum child file size to scan.
fortimail-expired on page 25	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 25	Set the timeout value to replay the request from FortiOS.
pending-jobs on page 26	This command allows users to view job queues statistics and purge them.
prescan-config on page 28	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 28	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 29	Turn adaptive scan on or off.
sandboxing-embeddedurl on page 30	Turn on or off sandboxing embedded URLs in PDF or Office documents. Only randomly selected URLs will be scanned.
sandboxing-parallel on page 31	Turn parallel scan on or off.
sandboxing-pipeline on page 31	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 32	Allow user to turn FortiGuard prefiltering on or off for certain file types.

sandboxing-ratio on page 33	Turn VM scan ratio on or off.
sandboxing-rse on page 33	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.
url-recheck on page 33	Enable/disable trusting previous scan results in Fortimail URL scan.

anti-phishing

Use this command to check URLs using the Real-time Zero-Day Anti-Phishing service. This feature is more sensitive for detecting phishing links compared with previous versions of URL detection.

This feature is editable on standalone and primary nodes only. On secondary and worker nodes, the enabled or disabled status is synchronized from the primary node. The settings may be different for each node depending on whether the contract valid or invalid.

Syntax

```
anti-phishing [-h|-l|-e|-d]
```

Option	Description
`-h (or --help)`	Help information.
`-l`	Display current Real-time Zero-Day Anti-Phishing Service setting
`-e`	Enable Real-time Zero-Day Anti-Phishing Service (default).
`-d`	Disable Real-time Zero-Day Anti-Phishing service

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.

Option	Description
`-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:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td><table><tr><th>Option</th><th>Description</th></tr><tr><td><code>-v</code></td><td>Set the single file size limitation, in megabytes (0 - 1024).</td></tr><tr><td><code>-u</code></td><td>Set the total uncompressed file size limitation for an archive file, in megabytes (0 - 2048).</td></tr></table></td></tr>
</table>

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).

ocr-scan

FortiSandbox includes a feature to detect text from images, though it is resource-intensive and is therefore disabled by default. You can use this CLI to enable or disable this functionality using the *ocr-scan* setting.

The configuration can be set/unset on standalone or primary unit.

In cluster mode, this setting is synchronized to all units in real time.

Syntax

```
ocr-scan [-h|-l|-e|-d]
```

Option	Description
`-h`	Help information.
`-l`	Display current OCR scan setting.
`-e`	Enable OCR scan on document files.
`-d`	Disable OCR scan on document files (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.

Option	Description
`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.
`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` • `url` • `android` • `mac` • `user` • `other`

prescan-config

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.

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 [-a|-b|-c|-h|-l|-n|-u]
```

Option	Description
`-a`	Set size limit (<100M) of the archive file that will be scanned with the executable file in VM (default 5M) While scanning executable child files inside a zip file, the zip file may be needed as well. This is because the executable child files may reference another file inside the zip file. FortiSandbox is able to pass the parent zip file into the VM along with the executable child file while it is scanning inside the VM. However, for performance reasons, the default maximum size of the parent zip that can be passed into the VM is 5M. You can modify this value to up to 100M if needed.
`-b`	Set big file (>512MB) unpack timeout in seconds (default = 600). The timeout value is applied to each individual file. For a big file, there is an overall hardcoded timeout of 3600 seconds. If timeout occurs when unpacking a file, it is put in the non-VM queue.
`-c`	Set maximum number of child files to extract from archive file (default = 1000). This maximum number is applied to the overall unpacking process of the top level archive file. The maximum depends on model.
`-h`	Help information.
`-l`	Show prescan settings.
`-n`	Set regular file (<=512MB) unpack timeout in seconds (default = 15). The timeout value is applied to each individual file. For a regular file, there is an overall hardcoded timeout of the number of files multiplied by 10 seconds. If timeout occurs when unpacking a file, it is put in the non-VM queue.
`-u`	Unset all prescan settings, that is, set to default.

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.
`-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-embeddedurl

Turn on or off sandboxing embedded URLs or QR code or executable file in PDF or Office or HTML 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.

Syntax

```
sandboxing-embeddedurl [-h|-e|-d|-i|-l|-t]
```

Option	Description
`-h`	Help information.
`-e`	Enable static scan and sandboxing on embedded URL/QR code/executable file.
`-d`	Disable sandboxing on embedded URL/QR code./executable file. If both static scan and sandboxing scan is disabled, you will need to need to run `-e` first, then `-d` to enable static scan and still disable sandboxing scan.
`-i`	Disable static scan and sandboxing on embedded URL/QR code/executable file.
`-l`	Display the scan status for embedded URL/QR code/executable file in PDF/Office/HTML documents.
`-t`	Type: • `url`: By default, static scan and sandboxing scan is enabled. • `qr`:By default, static scan is enabled, sandboxing scan is disabled. • `file`: By default, static scan is enabled, sandboxing scan is disabled. Only enable/disable either `url` or `qr` one at a time. For example, you cannot combine `-e -tqr -e -turl`.

Example:

To enable qrcode in static and sandboxing scan:

```
sandboxing-embeddedurl -e -tqr
```

Sample output:

```
Scan status for embedded QR codes in PDF, Office or HTML documents:
static scan of embedded QR codes: enabled
sandboxing of embedded QR codes: enabled
```

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.

Option	Description
`-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]`: Enable sandboxing prefilter for specific types.
`-d`	Disable sandboxing prefilter (default). - `-t [dll|pdf|swf|js|htm|url|office|trustvendor|trustdomain|archive|trustfndr]`: Enable 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.
`trustfndr`	Replace the `trustfai`.

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.

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.
`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.
`iptables`	Enable/disable IP tables.
`log-dropped`	Enable/disable the log file drop event.
`log-purge`	Delete all system logs.
`oftpd-con-mode`	Enable/disable conserve mode of OFTPD. For details, see oftpd-con-mode on page 45.
`ps-status`	Use this command to display power supply status.
`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.

Command	Description
`reset-sandbox-engine`	Reset the tracer/rating engine back to firmware default.
`reset-scan-profile`	Reset the scan flow settings to firmware default values.
`reset-widgets`	Reset the GUI widgets.
`restore-sysconf`	Restore system configuration from remote server. For details, see restore-sysconf on page 49.
`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.
`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
```

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]
```

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-a</code></td><td>Add a confirmation ID<table><tr><th>Option</th><th>Description</th></tr><tr><td><code>-k</code></td><td>License key or username from account information.</td></tr><tr><td><code>-c</code></td><td>Conformation ID.</td></tr><tr><td><code>-n</code></td><td>Name of VM.</td></tr></table></td></tr>
<tr><td><code>-d</code></td><td>Delete a confirmation ID.<table><tr><th>Option</th><th>Description</th></tr><tr><td><code>-k</code></td><td>License key or username from account information.</td></tr></table></td></tr>
<tr><td><code>-l</code></td><td>List all confirmation IDs.</td></tr>
</table>

Example

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

```
confirm-id -a -kSGWGG-J668H-X2VMG-6FBRW-XXXXX -
     c505186493511372501554005080163933500466920783662 -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|-i|-r|-b|-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.
`-i`	Enable In-Line Block on all FortiGate devices. By default, block setting for only malicious, high risk and medium risk.
`-r`	Disable In-Line Block on all FortiGate devices.
`-b`	Disable auto-enabling of In-Line Block on FortiGate devices.
`-l`	Display the status of device and FortiClient authorization. Default: manually.

Example

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

- Device authorization is automatic.
- FortiSandbox will authorize FortiClient automatically.
- Enable In-Line Block on all FortiGate devices. By default, block settings for only malicious, high risk and medium risk.

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 CBC cipher suite.
`-g`	Enable TLS 1.3 for devices (default).
`-f`	Disable TLS 1.3 (max 1.2) for devices.
`-j`	Disable CBC cipher suite for devices and GUI (default).

Option	Description
`-k`	Enable CBC cipher suite for devices and GUI .

Default settings:

Enable TLS 1.3 for devices

Enable CBC cipher suite for devices and GUI

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 when you want to remove sensitive data from the hard disk without delating the default Windows VMs. This saves times 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.

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

Before executing the CLI, please make sure the console is connected to set the password and IP.

This command is not available on VM appliances, or lower-end hardware appliance 500F.

This command is only allowed in Standalone mode.

Syntax

```
format-storage
```

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)
```

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]
```

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-h</td><td>Help information.</td></tr>
<tr><td>-b</td><td>Download an image file from this server and upgrade the firmware.</td></tr>
<tr><td>-v</td><td>Download a VM image file from this server and install.</td></tr>
<tr><td>-e</td><td>Download a system rating/tracer engine from this server and install.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-t&lt;ftp|https|scp&gt;</td><td>The protocol type, FTP/HTTPS/SCP. The default is scp.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-s&lt;SCP/FTP/HTTPS server IP address&gt;</td><td>Download an image file from this server IP address.</td></tr>
<tr><td>-u&lt;user name&gt;</td><td>The user name for authentication.</td></tr>
<tr><td>-f&lt;full path of filename&gt;</td><td>The full path for the image file.</td></tr>
<tr><td>-x[t|s|p|u|w]</td><td>Proxy server configuration.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-xt[http|socks4|socks5]</td><td>Proxy server type.</td></tr>
<tr><td>-xs</td><td>Proxy server IP or FQDN name.</td></tr>
<tr><td>-xp</td><td>Proxy server port.</td></tr>
<tr><td>-xu</td><td>Proxy server authentication username.</td></tr>
<tr><td>-xw</td><td>Proxy server authentication password.</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

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
   ```

iptables

This command is used to enable or disable IP tables. The settings will be discarded after reboot.

Syntax

```
iptables -[ACD] chain rule-specification [options]
iptables -I chain [rulenum] rule-specification [options]
iptables -R chain rulenum rule-specification [options]
iptables -D chain rulenum [options]
iptables -[LS] [chain [rulenum]] [options]
iptables -[FZ] [chain] [options]
iptables -[NX] chain
iptables -E old-chain-name new-chain-name
iptables -P chain target [options]
iptables -h (print this help information)
```

Commands

Either long or short commands are allowed.

Command	Description
`--append -A chain`	Append to chain.
`--check -C chain`	Check for the existence of a rule.
`--delete -D chain`	Delete matching rule from chain.
`--delete -D chain rulenum`	Delete rule rulenum (1 = first) from chain.
`--insert -I chain [rulenum]`	Insert in chain as rulenum (default 1=first).
`--replace -R chain rulenum`	Replace rule rulenum (1 = first) in chain.
`--list -L [chain [rulenum]]`	List the rules in a chain or all chains.
`--list-rules -S [chain [rulenum]]`	Print the rules in a chain or all chains.
`--flush -F [chain]`	Delete all rules in chain or all chains.
`--zero -Z [chain [rulenum]]`	Zero counters in chain or all chains.
`--new -N chain`	Create a new user-defined chain.
`--delete-chain -X [chain]`	Delete a user-defined chain.
`--policy -P chain target`	Change policy on chain to target.
`--rename-chain -E old-chain new-chain`	Change chain name, (moving any references).

Options

Either long or short options are allowed.

Option	Description
`--ipv4 -4`	Nothing (line is ignored by ip6tables-restore).
`--ipv6 -6`	Error (line is ignored by iptables-restore).
`[!] --protocol -p proto`	Protocol: by number or name, for example: `tcp`.
`[!] --source -s address [/mask][...]`	Source specification.
`[!] --destination -d address[/mask][...]`	Destination specification.
`[!] --in-interface -i input name[+]`	Network interface name ([+] for wildcard).
`--jump -j target`	Target for rule (may load target extension).
`--goto -g chain`	Jump to chain with no return.
`--match -m match`	Extended match (may load extension).
`--numeric -n numeric`	Output of addresses and ports.
`[!] --out-interface -o output name[+]`	Network interface name ([+] for wildcard).
`--table -t table`	Table to manipulate (default: `filter').
`--verbose -v`	Verbose mode.
`--wait -w`	Wait for the xtables lock.
`--line-numbers`	Print line numbers when listing.
`--exact -x`	Expand numbers (display exact values).
`[!] --fragment -f`	Match second or further fragments only.
`--modprobe=<command>`	Try to insert modules using this command.
`--set-counters PKTS BYTES`	Set the counter during insert/append.
`[!] --version -V`	Print package version.

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
```

oftpd-con-mode

Enable/disable conserve mode of OFTPD.

Syntax

```
oftpd-con-mode [-h|-l|-e|-d]
```

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

ps-status

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

Syntax

```
ps-status
```

raid-rebuild

Rebuild raid after a new HD replaces a bad one. This option is only available on hardware models.

Syntax

```
raid-rebuild [-h|-l|-d]
```

Option	Description
`-h`	Help information.
`-d[diskno]`	Rebuild RAID after the HD disk number is swapped.
`-l[diskno]`	Show the rebuild progress.

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|-b]
```

Option	Description
`-h`	Help information.
`-t`	Reset tracer engine to firmware default.
`-r`	Reset rating engine to firmware default.
`-b`	Reset both tracer and rating engines to firmware default.

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, 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-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 allowed TLS version for HTTPS service.

Syntax

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

Option	Description
`-h`	Help information.
`-l`	Show current TLS versions.
`-r`	Reset to default versions.
`-e[1|2|3]`	Set the allowed TLS versions. `1`, `2`, or `3` are for TLS 1.1, 1.2, or 1.3. Separate versions with `|`, for example `-e2|3` will enable TLS 1.2 and 1.3. The default is TLS 1.2 and 1.3. TLS 1.0 is 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.
- 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.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-c</code></td><td>Create an Administrator account.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-u</code></td><td>Administrator account name.</td></tr>
<tr><td><code>-p</code></td><td>Administrator account password
When the <i>System</i> > <i>Password Policy</i> is enabled, it will influence the <code>-p</code> parameter within this CLI command during the creation of local users.</td></tr>
<tr><td><code>-e</code></td><td>Email address</td></tr>
<tr><td><code>-o</code></td><td>Phone number</td></tr>
</table>
</td></tr>
</table>

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

Examples

Create a local Super Admin user:

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

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]
```

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-h</td><td>Help information.</td></tr>
<tr><td>-e</td><td>Enable the specified upload setting.</td></tr>
<tr><td>-d</td><td>Disable the specified upload setting.</td></tr>
<tr><td>-t[uploadcloud|submiturl|uploadstats]</td><td>Set the type of upload setting:
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>uploadcloud</td><td>Upload malicious and suspicious file information to Sandbox Community Cloud. Default is enabled.</td></tr>
<tr><td>submiturl</td><td>Submit suspicious URL to Fortinet WebFilter service. Default is disabled.</td></tr>
<tr><td>uploadstats</td><td>Upload statistics data to</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td><table><tr><th>Options</th><th>Description</th></tr><tr><td></td><td>FortiGuard service. Default is disabled.</td></tr></table></td></tr>
<tr><td><code>-l</code></td><td>Display the status of the upload settings</td></tr>
</table>

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>
```

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-h (or --help)</code></td><td>Help information.</td></tr>
<tr><td><code>-c[n|l|f|d|u]</code></td><td>Operation command.
<table>
<tr><th colspan="2">Option</th></tr>
<tr><td><code>n</code></td><td>Install a new customized VM.</td></tr>
<tr><td><code>l</code></td><td>List installed customized VM.</td></tr>
<tr><td><code>f</code></td><td>Upload a meta file for a customized VM.</td></tr>
<tr><td><code>d</code></td><td>Display a meta file for a customized VM.</td></tr>
<tr><td><code>u</code></td><td>Upload a VDI file to a remote server.
Supported protocols include TFTP, FTP, and SCP.</td></tr>
</table></td></tr>
<tr><td><code>-t&lt;ftp|scp|tftp&gt;</code></td><td>The protocol type, FTP, SCP (default) or tftp.</td></tr>
<tr><td><code>-s&lt;server IP&gt;</code></td><td>Download the image file from this FTP or SCP server IP address.</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-u&lt;user name&gt;</code></td><td>User name for authentication.</td></tr>
<tr><td><code>-f&lt;full path of filename&gt;</code></td><td>Full path for the image file or meta file.</td></tr>
<tr><td><code>-d&lt;hardware/machine ID&gt;</code></td><td>Original hardware ID or machine ID.</td></tr>
<tr><td><code>-k&lt;MD5 checksum&gt;</code></td><td>MD5 checksum for the uploaded file.</td></tr>
<tr><td><code>-v[o|n|c|m]</code></td><td>Set the base information for VM image
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>o&lt;OS type&gt;</code></td><td>Windows10, or Windows10_64,Windows11_64, Linux, Linux_64.</td></tr>
<tr><td><code>n&lt;VM name&gt;</code></td><td>Name of the VM.</td></tr>
<tr><td><code>c&lt;CPU&gt;</code></td><td>CPU number, 1-4</td></tr>
<tr><td><code>m&lt;Memory&gt;</code></td><td>Memory size in MB, 1024-4096</td></tr>
</table></td></tr>
<tr><td><code>-r &lt;VM name&gt;</code></td><td>Replace the VM if it already exists.</td></tr>
<tr><td><code>-m &lt;VM meta file name&gt;</code></td><td>Name of the VM meta file.</td></tr>
</table>

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]
```

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-h (or --help)</code></td><td>Help information.</td></tr>
<tr><td><code>-l</code></td><td>Display the current configuration.</td></tr>
<tr><td><code>-s</code></td><td>Set the VM internet configuration for port3.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-g&lt;gateway IP&gt;</code></td><td>Next hop gateway IP address.</td></tr>
<tr><td><code>-d&lt;DNS server IP&gt;</code></td><td>DNS server IP address.</td></tr>
</table></td></tr>
<tr><td><code>-u</code></td><td>Unset VM internet configuration for port3.</td></tr>
</table>

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.

Option	Description
`-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
2024-12-18	Initial release of v5.0.1
2024-02-25	Updated device-ssl on page 39.

www.fortinet.com