FORTINET
High Performance Network Security

FortiSandbox - CLI Reference Guide

VERSION 2.3.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

November 03, 2016

FortiSandbox 2.3.2 CLI Reference Guide

34-231-385491-20161103

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-11-03	Initial release.

CLI Reference Guide

The FortiSandbox has CLI commands that are accessed when accessing the FortiSandbox via console or by using a SSH or TELNET client. These services must be enabled on the port1 interface.

The FortiSandbox CLI commands are intended to be used for initial device configuration and troubleshooting. Some commands are specific to hardware or VM devices.

Use `-h` or `--help` with system commands for information on how to use the command. The FortiSandbox CLI is case-sensitive.

What's New in 2.3.2

Command	Description
`diagnose-debug`	Modified `diagnose-debug` to support adapter troubleshooting. Added the following: • `adapter_cb`: Daemon for third party device such as Bit9 + CARBON BLACK. • `adapter_icap`: Daemon for Internet Content Adaptation Protocol (ICAP)

`diagnose-sys-top`	Display current system top processes and current CPU/Memory usage.
	Usage:
	`diag-sys-top [-h|-l|-i]`
	`-h Help information.`
	`-l <value> Maximum lines (default 50, maximum 100)`
	`-i <value> Interval to delay in seconds (default 5)`

`diagnose-sys-perf`	Display system performance information.
	Usage:
	`diagnose-sys-perf [-h|-m]`
	`-h Help information.`
	`-m<value> Last hours (default 1 hour, maximum 4 weeks (40320 hours).`

CLI Commands

General commands

Command	Description
`help`	Display list of valid CLI commands. Privilege: Full access only.
`?`	You can also enter `?` for help. Privilege: Full access only.
`exit`	Terminate the CLI session. Privilege: Full access and Read-only.

Configuration commands

Command	Description

`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 sniffer, it will not be displayed.
	Example:
	`show`
	`Configured parameters:`
	`Port 1 IPv4 IP: 172.16.69.32/24 MAC: 0C:C4:7A:54:EB:5C`
	`Port 1 IPv6 IP: 2620:101:9005:69::32/64 MAC: 0C:C4:7A:54:EB:5C`
	`Port 2 IPv4 IP: 182.16.70.32/24 MAC: 0C:C4:7A:54:EB:5D`
	`Port 3 IPv4 IP: 192.168.199.32/24 MAC: 0C:C4:7A:54:EB:5E`
	`Port 4 IPv4 IP: 4.0.0.3/24 MAC: 0C:C4:7A:54:EB:5F`
	`Port 4 IPv6 IP: 4101::4/64 MAC: 0C:C4:7A:54:EB:5F`
	`IPv4 Default Gateway: 172.16.69.1`
	Privilege: Full access and Read-only

Command	Description

`set`	Set configuration parameters. The available attributes/values for `set` are:
	`port1-ip <IP/netmask>`
	`e.g. port1-ip 1.2.3.4/24`
	`port2-ip <IP/netmask>`
	`e.g. port2-ip 1.2.3.4/24`
	`port3-ip <IP/netmask>`
	`e.g. port3-ip 1.2.3.4/24`
	`port4-ip <IP/netmask>`
	`e.g. port4-ip 1.2.3.4/24`
	`port5-ip <IP/netmask>`
	`e.g. port5-ip 1.2.3.4/24`
	`port6-ip <IP/netmask>`
	`e.g. port6-ip 1.2.3.4/24`
	`port7-ip <IP/netmask>`
	`e.g. port7-ip 1.2.3.4/24`
	`port8-ip <IP/netmask>`
	`e.g. port8-ip 1.2.3.4/24`
	`default-gw <IP>`
	`date <YYYY-MM-DD>`
	`time <HH:MM:SS>`
	Privilege: Full access only

`unset`	Unset configuration parameters. The available attribute for `unset` is `default-gw`. Privilege: Full access only

System commands

Command	Description
`reboot`	Reboot the FortiSandbox. All sessions will be terminated. The unit will go off-line and there will be a delay while it restarts. `-f` to force an immediate reboot. Privilege: Full access only.
`config-reset`	Reset the FortiSandbox configuration to factory default settings. Job data will be kept. For installed VM images, their clone numbers and *Scan Profile* settings are set back to default. Privilege: Full access only.

`factory-reset`	Reset FortiSandbox configuration to factory default settings, delete all data. For installed VM images, only Default VMs are kept and their clone number and *Scan Profile* settings are set back to default.
	Example:
	`factory-reset`
	`This command will erase your current configuration and all stored data.`
	`Do you want to continue? (y/n)`
	`Enter y to continue.`
	Privilege: Full access only.

Command	Description

shutdown	Shut down the FortiSandbox.
	Example:
	`shutdown`
	`Do you want to continue? (y/n)`
	`Enter y to continue.`
	Privilege: Full access only.

status	Display the FortiSandbox firmware version, serial number, system time, disk usage, image status check, Microsoft Windows VM status, VM network access configuration, and RAID information.
	Example:
	`status`
	`System:`
	`Version: v2.20-build0143 (GA)`
	`Serial number: FSA3KD3R00000009`
	`System time: Wed Mar 18 10:57:35 2016`
	`Disk Usage: 780 GB`
	`Image status check: OK`
	`Windows VM: Activated and Initialized`
	`VM Internet access: On`
	`RAID Info:`
	`RAID level: Raid-1`
	`RAID status: OK`
	`Virtual drive size: 3 GB`
	`Total physical disks: 4`
	`Physical disk states:`
	`Slot: 0`
	`Status: Unavailable`
	`Size: 0 GB`
	`Slot: 1`
	`Status: Unavailable`
	`Size: 0 GB`
	`Slot: 2`
	`Status: Unavailable`
	`Size: 0 GB`
	`Slot: 3`
	`Status: Unavailable`
	`Size: 0 GB`
	`Slot: 4`
	`Status: OK`
	`Size: 1862 G`
	Privilege: Full access and Read-only.

sandbox-engines	Display FortiSandbox FortiGuard component versions including the Tracer Engine, Rating Engine, Traffic Sniffer, Botnet Signature Database, and IPS Signature Database, and Android engine versions.
	Example:
	`sandbox-engines`
	`Sandbox components versions:`
	`Tracer Engine: 02003.00267`
	`Rating Engine: 02003.00251`
	`Traffic Sniffer: 00003.00279`
	`Network Alerts Signature: 00002.01103`
	`Android Analytic Engine: 02003.00012`
	`Android Rating Engine: 02003.00012`
	Privilege: Full access only.

Command	Description
sandboxing-cache	User can turn on/off the Sandboxing result cache. When it is off, the same file will be scanned again by Sandboxing.
fw-upgrade	Upgrade or re-install the FortiSandbox firmware via an Secure Copy (SCP) or File Transfer Protocol (FTP) server. Before running this command, the firmware file should be downloaded to a server that supports file copy with the FTP/SCP command. Usage: fw-upgrade -h -h Help information. -l Install a VM image file from a local server. -b Download an image file from this server and upgrade the firmware. -v Download a VM image file from this server and install. -s<SCP/FTP server IP address> Download an image file from this server IP address. -u<user name> The user name for authentication. -p<password> The password for authentication. -f/<full path of filename> The full path for the image file. -t<ftp | scp> The protocol type, FTP or SCP. The default is SCP. The system will boot up after firmware is downloaded and installed. Privilege: Full access only.
cleandb	Clean up the internal database and job information.
log-purge	This command will delete all your system logs. You will be prompted to confirm this action. Example: log-purge This command will delete all your system logs. Do you want to continue? (y/n) Enter y to continue. Privilege: Full access only.

Command	Description

pending-jobs	This command allows users to view the statistics of job queues and purge them
	`pending-jobs show|purge source filetype`
	Source:
	`<all|ondemand|rpc|device|sniffer|adapter|netshare|url|urlrpc|urldev|urladapter>`
	Specifically:
	• `url` means URLs submitted through the On Demand page.
	• `urlrpc` means URLS submitted through JSON API.
	• `urldev` means URLs submitted from devices such as FortiMail.
	Filetype:
	`<all|exe|pdf|doc|flash|web|url|notset|waiting>`
	Specifically:
	• `notset` means jobs wont be scanned by guest image
	• `waiting` means files have not been processed to enter the job queue.
	Example:
	`pending-jobs show sniffer all`
	`Source: Sniffer, File type: Microsoft Office files (Word, Excel, PowerPoint files etc), Jobs: 0`
	`Source: Sniffer, File type: Adobe Flash files, Jobs: 5`
	`Source: Sniffer, File type: Executables/VBS/BAT/PS1/JAR/MSI files, Jobs: 3`
	`Source: Sniffer, File type: Customer defined files, Jobs: 0`
	`Source: Sniffer, File type: Android files, Jobs: 0`
	`Source: Sniffer, File type: PDF files, Jobs: 3`
	`Source: Sniffer, Queued Jobs: 0`
	`Source: Sniffer, Non-VM Jobs: 0`
	`Source: Sniffer, Not assigned jobs: 0`
	`Source: Sniffer, Total Jobs: 0`
	`Total Jobs: 0`

Command	Description

iptables	This command is used to enable or disable IP tables. The settings will be discarded after reboot.
	Usage:
	`iptables -[AD] 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 -6 Enable or disable IPv6 tables`
	`iptables -h (print this help information)`
	Privilege: Full access only.

vm-license	List or re-install embedded licenses for FortiSandbox Windows VM. Use '-h' for more information.
	Usage:
	`-h Help information.`
	`-l List the Windows Product key information.`
	`-b Download a file from server and burn the Windows Product keys to system.`
	`-t <scp | tftp | ftp> Specify the protocol. scp: download via SCP. tftp: download via TFTP. The default is tftp.`
	`-s <server ip> Download the license key file from this IP address. The default port for TFTP is 69.`
	`-u <user name> The user name for server authentication.`
	`-p <password> The password for server authentication.`
	`-f <filename> The name of the license key file.`
	Example:
	`vm-license -l`
	`28 keys in total`
	`KEY_WINXP XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`
	`.....`
	`KEY_WIN7 XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`
	`.....`
	`Windows Product Keys Validation .......... Passed`
	Privilege: Full access only.

Command	Description

vm-status	Show FortiSandbox VM system status.
	Example:
	`vm-status`
	`WIN7X86VM was activated and initialized`
	`WINXPVM was activated and initialized`
	`WIN10X64VM was activated and initialized`
	`WIN7X64VM was activated and initialized`
	`Virtual Hosts Initialization .......... Passed`
	
	`Installed VM Images:`
	`ID Ver Name License (App Status)`
	`4 6 WINXPVM1 Permanent Office 2010 (activated)`
	`1 7 WINXPVM Permanent Office 2007 (activated)`
	`64 1 WIN7X86VMIchi Permanent`
	`8 6 WIN7X86VM Permanent Office 2013 (activated)`
	`2 7 WIN7X64VM Permanent`
	`1024 1 WIN10X86VM nokey`
	`512 1 WIN10X64VM nokey`
	If there is an issue with the FortiSandbox VM, an error message will be displayed with information on troubleshooting the problem.
	Privilege: Full access only.

vm-reset	Activate and initialize a VM image again. Sometimes it is necessary to rebuild a VM image when it is broken.
	
	Usage:
	`-h Help information.`
	`-n VM name.`

device-authorization	Users can decide to either manually or automatically authorize a new client device.
	Usage:
	`device-authorization -[h|a|m|l]`
	`-h Help information.`
	`-a When a new device registers, FortiSandbox will authorize it automatically.`
	`-m When a new device registers, the user has to authorize it manually from the WebUI.`
	`-l Display the status of device authorization. Default: manually.`

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.
	Usage:
	`-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 be regular one.`

Command	Description

hc-settings	Configure the unit as a HA-Cluster mode unit.
	Usage:
	`-h Help information.`
	`-l List the Cluster configuration.`
	`-sc Set this unit to be a HA-Cluster mode unit.`
	`-t<N|M|P|R> Set this unit to be a HA-Cluster mode unit.`
	`N: N/A`
	`M:Master unit`
	`P:Primary slave unit`
	`R:Regular slave unit`
	`-n<name string> Set alias name for this unit.`
	`-c<HA-CLUSTER name> Set the HA-Cluster name for Master unit.`
	`-p<authentication code> Set the authentication code for Master unit.`
	`-i<interface> Set interface used for cluster internal communication.`
	`-si Set the fail-over IPs for this cluster for Master unit.`
	`-i<interface> Specify the interface for external communication`
	`-a<IP/netmask> Specify the IP address and netmask for external communication. This IP address will be 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.`

hc-status	List the status of HA-Cluster units.
	Usage:
	`-h Help information.`
	`-l List the status of HA-Cluster units.`

hc-slave	Add/Update/Remove a slave unit to/from HA Cluster.
hc-master	Disable/Enable the malware detection features on master unit. When `-s` is used, the user can turn on the file scan and determine the percentage of the scanning capacity to be used. If no number follows the `-s`, 50% will be used (half of the processing capacity will be used).

confirm-id	Validate a Microsoft Windows or Office key after contacting Microsoft customer support. For more details, please contact Fortinet Customer Support.
	Usage:
	`-a Add a confirmation ID.`
	`-k License key.`
	`-c Confirmation ID.`
	`-d Delete a confirmation ID.`
	`-k License key.`
	`-l List all confirmation IDs.`

Command	Description

remote-auth-timeout	Set Radius or LDAP authentication timeout value.
	Usage:
	`-h Help information.`
	`-s Set timeout value to 10 to 180 seconds`
	`-u Unset timeout`
	`-l Display timeout value`

filesize-limit	Set file size limit of different input sources.
	Usage:
	`filesize-limit [-h|-l|-t] -t [all|ondemand|netshare|jsonrpc] -v200`
	`-h Help information.`
	`-l Display the file size limitations.`
	`-t[all|ondemand|netshare|jsonrpc]`
	`-v[file size limitation (MBytes)] (0 < size < 1024)`

log-dropped	Enable the log file drop event.
	Usage:
	`log-dropped [-h|-l|-e|-d]`
	`-h Help information.`
	`-l Show current config.`
	`-e Enable log dropped file.`
	`-d Disable log dropped file.`

Utilities

Command	Description
ping	Test network connectivity to another network host. Usage: `ping <IP address>` Privilege: Full access only.
tcpdump	Examine local network traffic. Usage: `tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX] [-B size] [-c count] [-C file_size] [-E algo:secret] [-F file] [-G seconds] [-i interface] [-j tstamptype] [-M secret] [-r file] [-s snaplen] [-T type] [-V file] [-w file] [-W filecount] [-y datalinktype] [-z command] [-Z user] [expression]` Privilege: Full access only.
traceroute	Examine the route taken to another network host. Usage: `traceroute <IP address>` Privilege: Full access only.

Command	Description

vm-customized	Install a new customized VM image
	Usage:
	`vm-customized`
	`-h Help information.`
	`-c command.`
	`-cn Install a new customized VM.`
	`-cl List installed customized VMs.`
	`-cf Upload a meta file for a customized VM.`
	`-cd Display a meta file for a customized VM.`
	`-t<ftp|scp> The protocol type, FTP or SCP. The default is scp.`
	`-s<SCP/FTP server IP address> Download an image file from this server IP address.`
	`-u<user name> The user name for authentication.`
	`-p<password> The password for authentication.`
	`-f<full path of filename> The full path for the image file.`
	`-o<OS type> WindowsXP Windows7 Windows7_64 Windows81 Windows81_64 Windows10 Windows10_64`
	`-v<VM name>`
	`-r Replace VM if it exists`
	
	Example: To install a new customized image hosted on a ftp server, execute the following command to install it:
	`vm-customized -cn –tftp –s<ftp_server_ip> -u<username> -p<password> -f</vdi_file_path> -o<Windows_type> –v<custom_vm_name>`

reset-scan-profile	Reset clone # and file extension association of VM images to default values.
	Usage:
	`reset-scan-profile`
	`-h Help information. -`
	`-r Reset clone # and file extension association.`

Command	Description

`sandboxing-prefilter`	Allow user to turn on/off pre-filtering of certain file types. If a file type is associated with a guest VM image, it will be scanned by it if the file type enters the job queue as defined in the Scan Profile page. The user can turn on pre-filtering of a file type so a file of such type will be statically scanned first by an advanced analytic engine and only suspicious ones will be sandboxing scanned by the guest image. This can improve the system's scan performance, but all files will still go through an AV scan, static scan, and community cloud query steps. For the URL type, when its pre-filtering is enabled, only URLs whose web filtering rating is Unrated will be scanned inside associated guest VM image.
	
	Usage:
	`sandboxing-prefilter [-h|-l|-e|-d] -t [dll|pdf|swf|js|htm|url|office]`
	`-h Help information.`
	`-e Enable sandboxing prefilter.`
	`-t[dll|pdf|swf|js|htm|url|office] Enable sandboxing prefilter for specific file types.`
	`-d Disable sandboxing prefilter.`
	`-t[dll|pdf|swf|js|htm|url|office] Disable sandboxing prefilter for specific file types.`
	`-l Display the status of sandboxing prefilter.`

`sandboxing-embeddedurl`	Allow user to turn on/off Sandboxing scan inside URLs of PDF and Office documents along with these files. Only randomly selected URLs will be scanned.
	Usage:
	`sandboxing-embeddedurl [-h|-l|-e|-d]`
	`-h Help information.`
	`-e Enable sandboxing embedded url in PDF or Office documents.`
	`-d Disable status for sandboxing embedded url.`
	`-l Display the status of sandboxing prefilter.`

Diagnostics

Command	Description
`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. Usage: `diagnose-debug [netshare|device|adapter -cb|adapter_icap][device_serial_number]` Where: • `netshare`: Network share deamon • `device`: OFTP daemon for FortiGate, FortiMail, and FortiClient devices. • `adapter_cb`: Daemon for third party device such as Bit9 + CARBON BLACK. • `adapter_icap`: Daemon for Internet Content Adaptation Protocol (ICAP).

`diagnose-sys-top`	Display current system top processes and current CPU/Memory usage.
	Usage:
	`diag-sys-top [-h|-l|-i]`
	`-h Help information.`
	`-l <value> Maximum lines (default 50, maximum 100).`
	`-i <value> Interval to delay in seconds (default 5).`

`diagnose-sys-perf`	Display system performance information.
	Usage:
	`diagnose-sys-perf [-h|-m]`
	`-h Help information.`
	`-m<value> Last hours (default 1 hour, maximum 4 weeks (40320 hours).`

`hardware-info`	Display general hardware status information. Use this command to view CPU, memory, disk, and RAID information, and system time settings. Privilege: Full access only.
`disk-attributes`	Display system disk attributes. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
`disk-errors`	Display any system disk errors. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.

Command	Description
`disk-health`	Display disk health information. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
`disk-info`	Display disk hardware status information. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
`raid-hwinfo`	Display RAID hardware status information. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
`test-network`	Test the network connection. The output can be used to detect network speed and connection to FDN servers and Microsoft servers.

FORTINET®

High Performance Network Security