

FortiSandbox - CLI Reference Guide

VERSION 2.3.0



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



August 30, 2016

FortiSandbox 2.3.0 CLI Reference Guide

34-230-385491-20160830

TABLE OF CONTENTS



Change Log	4
CLI Reference Guide	5

Change Log

Date	Change Description
2016-08-30	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.

General commands

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

Configuration commands

Command	Description
<code>show</code>	<p>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.</p> <p>Example:</p> <pre> 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 </pre> <p>Privilege: Full access and Read-only</p>

Command	Description
set	<p>Set configuration parameters. The available attributes/values for <code>set</code> are:</p> <pre> 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> </pre> <p>Privilege: Full access only</p>
unset	<p>Unset configuration parameters. The available attribute for <code>unset</code> is <code>default-gw</code>.</p> <p>Privilege: Full access only</p>

System commands

Command	Description
reboot	<p>Reboot the FortiSandbox. All sessions will be terminated. The unit will go offline and there will be a delay while it restarts. <code>-f</code> to force an immediate reboot.</p> <p>Privilege: Full access only.</p>
config- reset	<p>Reset the FortiSandbox configuration to factory default settings. Job data will be kept. For installed VM images, their clone numbers and <i>Scan Profile</i> settings are set back to default.</p> <p>Privilege: Full access only.</p>
factory- reset	<p>Reset FortiSandbox configuration to factory default settings, delete all data. For installed VM images, only Default VMs are kept and their clone number and <i>Scan Profile</i> settings are set back to default.</p> <p>Example:</p> <pre> factory-reset This command will erase your current configuration and all stored data. Do you want to continue? (y/n) Enter y to continue. </pre> <p>Privilege: Full access only.</p>

Command	Description
shutdown	<p>Shut down the FortiSandbox.</p> <p>Example:</p> <pre>shutdown Do you want to continue? (y/n) Enter y to continue.</pre> <p>Privilege: Full access only.</p>
status	<p>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.</p> <p>Example:</p> <pre>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</pre> <p>Privilege: Full access and Read-only.</p>

Command	Description
sandbox-engines	<p>Display FortiSandbox FortiGuard component versions including the Tracer Engine, Rating Engine, Traffic Sniffer, Botnet Signature Database, and IPS Signature Database, and Android engine versions.</p> <p>Example:</p> <pre>sandbox-engines Sandbox components versions: Tracer Engine: 5.0.576 Rating Engine: 2.1.085 Traffic Sniffer: 3.1.164 Botnet Signature DB: 2.825 IPS Signature DB: 7.817 Android Analytic Engine: 003 Android Rating Engine: 1.0.0</pre> <p>Privilege: Full access only.</p>
sandboxing-cache	<p>User can turn on/off the Sandboxing result cache. When it is off, the same file will be scanned again by Sandboxing.</p>
fw-upgrade	<p>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.</p> <p>Usage:</p> <pre>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.</pre> <p>The system will boot up after firmware is downloaded and installed.</p> <p>Privilege: Full access only.</p>
cleandb	<p>Clean up the internal database and job information.</p>

Command	Description
log-purge	<p>This command will delete all your system logs. You will be prompted to confirm this action.</p> <p>Example:</p> <pre>log-purge This command will delete all your system logs. Do you want to continue? (y/n) Enter y to continue.</pre> <p>Privilege: Full access only.</p>
pending-jobs	<p>This command allows users to view the statistics of job queues and purge them</p> <pre>pending-jobs show purge source filetype</pre> <p>Source:</p> <pre><all ondemand rpc device sniffer adapter netshare url urlrpc urldev urladapter></pre> <p>Specifically:</p> <ul style="list-style-type: none"> • 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. <p>Filetype:</p> <pre><all exe pdf doc flash web url notset waiting></pre> <p>Specifically:</p> <ul style="list-style-type: none"> • notset means jobs wont be scanned by guest image • waiting means files have not been processed to enter the job queue. <p>Example:</p> <pre>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</pre>

Command	Description
iptables	<p>This command is used to enable or disable IP tables. The settings will be discarded after reboot.</p> <p>Usage:</p> <pre>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)</pre> <p>Privilege: Full access only.</p>
vm-license	<p>List or re-install embedded licenses for FortiSandbox Windows VM. Use '-h' for more information.</p> <p>Usage:</p> <pre>-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.</pre> <p>Example:</p> <pre>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</pre> <p>Privilege: Full access only.</p>

Command	Description
vm-status	<p>Show FortiSandbox VM system status.</p> <p>Example:</p> <pre>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</pre> <p>If there is an issue with the FortiSandbox VM, an error message will be displayed with information on troubleshooting the problem.</p> <p>Privilege: Full access only.</p>
vm-revert	Revert VM images back to the point of the last fw-upgrade -v execution.
vm-reset	<p>Activate and initialize a VM image again. Sometimes it is necessary to rebuild a VM image when it is broken.</p> <p>Usage:</p> <pre>-h Help information. -n VM name.</pre>
device-authorization	<p>Users can decide to either manually or automatically authorize a new client device.</p> <p>Usage:</p> <pre>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.</pre>
usg-license	<p>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.</p> <p>Usage:</p> <pre>-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.</pre>

Command	Description
hc-settins	<p>Configure the unit as a HA-Cluster mode unit.</p> <p>Usage:</p> <ul style="list-style-type: none"> -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. <ul style="list-style-type: none"> 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	<p>List the status of HA-Cluster units.</p> <p>Usage:</p> <ul style="list-style-type: none"> -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	<p>Disable/Enable the malware detection features on master unit.</p> <p>When <code>-s</code> 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 <code>-s</code>, 50% will be used (half of the processing capacity will be used).</p>
confirm-id	<p>Validate a Microsoft Windows or Office key after contacting Microsoft customer support. For more details, please contact Fortinet Customer Support.</p> <p>Usage:</p> <ul style="list-style-type: none"> -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	<p>Set Radius or LDAP authentication timeout value.</p> <p>Usage:</p> <ul style="list-style-type: none"> -h Help information. -s Set timeout value to 10 to 180 seconds -u Unset timeout -l Display timeout value
filesize-limit	<p>Set file size limit of different input sources.</p> <p>Usage:</p> <pre>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)</pre>
log-dropped	<p>Enable the log file drop event.</p> <p>Usage:</p> <pre>log-dropped [-h -l -e -d] -h Help information. -l Show current config. -e Enable log dropped file. -d Disable log dropped file.</pre>

Utilities

Command	Description
ping	<p>Test network connectivity to another network host.</p> <p>Usage:</p> <pre>ping <IP address></pre> <p>Privilege: Full access only.</p>
tcpdump	<p>Examine local network traffic.</p> <p>Usage:</p> <pre>tcpdump [-aAbdDefhHIJKlLnOpqRStuUvX] [-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]</pre> <p>Privilege: Full access only.</p>
traceroute	<p>Examine the route taken to another network host.</p> <p>Usage:</p> <pre>traceroute <IP address></pre> <p>Privilege: Full access only.</p>

Command	Description
vm-customized	<p>Install a new customized VM image</p> <p>Usage:</p> <pre>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</pre> <p>Example: To install a new customized image hosted on a ftp server, execute the following command to install it:</p> <pre>vm-customized -cn -tftp -s<ftp_server_ip> - u<username> -p<password> -f</vdi_file_ path> -o<Windows_type> -v<custom_vm_name></pre>
reset-scan-profile	<p>Reset clone # and file extension association of VM images to default values.</p> <p>Usage:</p> <pre>reset-scan-profile -h Help information. - -r Reset clone # and file extension association.</pre>

Command	Description
<code>sandboxing-prefilter</code>	<p>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 non-suspicious files will not be scanned. It will be statically scanned first by an advanced analytic engine and 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.</p> <p>Usage:</p> <pre>sandboxing-prefilter [-h -l -e -d] -t [dll pdf swf js htm url] -h Help information. -e Enable sandboxing prefilter. -t[dll pdf swf js htm url] Enable sandboxing prefilter for specific file types. -d Disable sandboxing prefilter. -t[dll pdf swf js htm url] Disable sandboxing prefilter for specific file types. -l Display the status of sandboxing prefilter.</pre>
<code>sandboxing-embeddedurl</code>	<p>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.</p> <p>Usage:</p> <pre>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.</pre>

Diagnostics

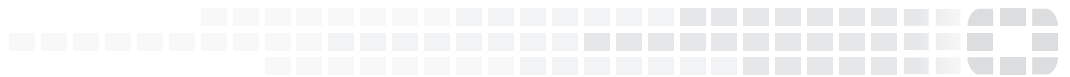
Command	Description
<code>diagnose-debug</code>	<p>Display detailed debug logs of network share scan and communications with devices. It is useful for troubleshooting OFTP and network share scan issues.</p> <p>Usage:</p> <pre>diagnose-debug [netshare device adapter] [device_ serial_number]</pre> <p>Where:</p> <ul style="list-style-type: none"> <code>netshare</code>: Network share daemon <code>device</code>: OFTP daemon for FortiGate, FortiMail, and FortiClient devices. <code>adapter</code>: Daemon for third party device such as Bit9 + CARBON BLACK.

Command	Description
<code>hardware-info</code>	Display general hardware status information. Use this command to view CPU, memory, disk, and RAID information, and system time settings. Privilege: Full access only.
<code>disk-attributes</code>	Display system disk attributes. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
<code>disk-errors</code>	Display any system disk errors. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
<code>disk-health</code>	Display disk health information. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
<code>disk-info</code>	Display disk hardware status information. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
<code>raid-hwinfo</code>	Display RAID hardware status information. Privilege: Full access only. This CLI command is available on hardware-based FortiSandbox models only.
<code>test-network</code>	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



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.