

# FortiSandbox - CLI Reference Guide

Version 2.5.1

**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](mailto:techdocs@fortinet.com)



January 17, 2018

FortiSandbox 2.5.1 CLI Reference Guide

34-251-455570-20180117

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
<b>What's New in FortiSandbox 2.5.1</b> .....	<b>7</b>
<b>Configuration Options</b> .....	<b>8</b>
show .....	8
set .....	8
unset .....	9
<b>System Options</b> .....	<b>10</b>
reboot .....	10
config-reset .....	10
factory-reset .....	10
shutdown .....	11
status .....	11
sandbox-engines .....	12
sandboxing-cache .....	12
fw-upgrade .....	13
cleandb .....	13
log-purge .....	13
pending-jobs .....	14
iptables .....	15
vm-license .....	15
vm-status .....	16
vm-reset .....	16
vm-internet .....	17
device-authorization .....	17
usg-license .....	18
resize-hd .....	18
upload-license .....	18
hc-settings .....	19
hc-status .....	20
hc-slave .....	20
hc-master .....	20
cm-status .....	21
confirm-id .....	21
remote-auth-timeout .....	22
filesize-limit .....	22
log-dropped .....	22
reset-widgets .....	23

---

fortimail-expired .....	23
raid-rebuild .....	24
set-maintainer .....	24
set-tlsver .....	24
reset-sandbox-engine .....	25
<b>Utility Commands .....</b>	<b>26</b>
ping .....	26
tcpdump .....	26
traceroute .....	26
vm-customized .....	26
reset-scan-profile .....	28
sandboxing-prefilter .....	28
sandboxing-embeddedurl .....	29
<b>Diagnose Options .....</b>	<b>31</b>
diagnose-debug .....	31
diagnose-sys-top .....	31
diagnose-sys-perf .....	32
disk-attributes .....	32
disk-errors .....	33
disk-health .....	33
disk-info .....	33
raid-hwinfo .....	33
test-network .....	34
<b>Glossary .....</b>	<b>35</b>
<b>Index .....</b>	<b>47</b>

## Change Log

Date	Change Description
2018-01-17	Initial release.

# Introduction

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 Options 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.

---



User's privilege to execute CLI commands is defined by user's admin profile. If user's admin profile has JSON API /CLI enabled, all CLI commands can be executed by the user. Otherwise only a very limited set of CLI commands are available.

---

# What's New in FortiSandbox 2.5.1

The following tables list the commands and variables that have changed in the CLI.

Command	Description
<code>oftpd-con-mode</code>	<p>Enable/disable unit to enter conserve mode to reject file submission from client devices (FGT/FML/FCT).</p> <p>Usage:</p> <pre>oftpd-con-mode -h Help information -e Enable OFTP daemon to enter conserve mode when an unprocessed   file number on the unit reaches 100,000. In a cluster   environment, OFTP daemon on the Master unit will enter   conserve mode when the average unprocessed file number on   each unit reaches 100,000. When the unit enters conserve   mode, it will reject file submissions from client devices.   The unit will exit conserve mode when unprocessed file   number becomes lower than 90,000. -d OFTP daemon will not enter conserve mode. This is the default   mode. -l Show current setting</pre>

# Configuration Options

## 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.

### syntax

```
show
```

### 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
```

## set

Set configuration parameters. The available attributes/values for `set` are:

### syntax

```
set
```

### example

```
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>
```

## unset

Unset configuration parameters.

### syntax

```
unset default-gw
```

# System Options

## reboot

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

### syntax

```
reboot
  -f
```

## 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.

### syntax

```
config-reset
```

## 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.

### syntax

```
factory-reset
```

### example

```
factory-reset
This Option will erase your current configuration and all stored data.
Do you want to continue? (y/n)
Enter y to continue.
```

## shutdown

Shut down FortiSandbox.

### syntax

```
shutdown
```

### example

```
shutdown
Do you want to continue? (y/n)
Enter y to continue.
```

## 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.

### syntax

```
status
```

### 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
```

## 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.

### syntax

```
sandbox-engines
```

### example

```
sandbox-engines
Sandbox components versions:
Sandbox Tracer Engine: 02005.00503
Sandbox Rating Engine: 02005.00504
Sandbox System Tools: 02005.00427
Traffic Sniffer: 00003.00432
Network Alerts Signature: 00002.01368
Android Analytic Engine: 02003.00013
Android Rating Engine: 02003.00013
```

## sandboxing-cache

User can turn on/off the Sandboxing result cache. When it is off, the same file will be scanned again by Sandboxing.

### syntax

```
sandboxing-cache
```

Option	Description
-h	Help information.
-e	Enable sandboxing result cache.
-d	Disable sandboxing result cache.
-l	Display the status of sandboxing result cache.
-r	Remove all existing cache results

## fw-upgrade

Upgrade or re-install the FortiSandbox firmware via an Secure Copy (SCP) or File Transfer Protocol (FTP) server. Before running this Option, the firmware file should be downloaded to a server that supports file copy with the FTP/SCP Option.

The system will boot up after firmware is downloaded and installed.

### syntax

fw-upgrade

Option	Description
-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

## cleandb

Clean up the internal database and job information.

### syntax

cleandb

## log-purge

This Option will delete all your system logs. You will be prompted to confirm this action.

## syntax

```
log-purge
```

### example

```
log-purge
This Option will delete all your system logs.
Do you want to continue? (y/n)
Enter y to continue.
```

## pending-jobs

This Option allows users to view the statistics of job queues and purge them

### syntax

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

### Source:

```
<all|ondemand|rpc|device|sniffer|adapter|netshare|url|urlrpc|urldev|urladapter|urlsniffer>
```

### 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.
- `urlsniffer` means URLs embedded in email body that are detected by sniffer.

### Filetype:

```
<all|exe|pdf|doc|flash|web|url|android|mac|user|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
```

## iptables

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

### syntax

```
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)
```

## vm-license

List or re-install embedded licenses for FortiSandbox Windows VM. Use '-h' for more information.

### syntax

```
vm-license
```

Option	Description
-h	Help information.
-l	List the Windows Product key information.

### example

```
vm-license -l
 28 keys in total
KEY_WINXP XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX
.....
KEY_WIN7 XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX
.....
Windows Product Keys Validation ..... Passed
```

## vm-status

Show FortiSandbox VM system status.

If there is an issue with the FortiSandbox VM, an error message will be displayed with information on troubleshooting the problem.

### syntax

```
vm-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 WIN7X86VM Ichi Permanent
8 6 WIN7X86VM Permanent Office 2013 (activated)
2 7 WIN7X64VM Permanent
1024 1 WIN10X86VM nokey
512 1 WIN10X64VM nokey
4294967306 0 MACOSX Trial
```

## vm-reset

Activate and initialize a VM image again. Sometimes it is necessary to rebuild a VM image when it is broken.

### syntax

```
vm-reset
```

Option	Description
-h	Help information.
-n	VM name.



## vm-internet

### syntax

```
vm-internet
```

Option	Description
-h	Help information.
-l	Display current configuration.
-s	Set VM internet configuration for port3.
-g	<gateway IP> Next hop gateway IP address.
-d	<DNS server IP> DNS server IP address.
-u	Unset VM internet configuration for port3.

### example

```
vm-internet -s -g192.168.199.1 -d8.8.8.8
```

## device-authorization

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

### syntax

```
device-authorization
```

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, the user has to authorize it manually from the WebUI.
-e	Authorize all existing devices if they are not already.
-o	When a new FortiClient registers, it inherits authorization status from the managing EMS or FGT. or the user has to change it manually from the WebUI.

Option	Description
-f	When a new FortiClient registers, FortiSandbox will authorize it automatically.
-l	Display the status of device and FortiClient authorization. (Default= manual).

## 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

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 be regular one.

## resize-hd

Available for FSA\_VM-Base and FSAVM00 model only.

After the user changes the virtual hard disk size on the hypervisor, the user should execute this Option to make the change recognizable to the firmware.

### syntax

resize-hd

## upload-license

Available for FSA-VM-Base and FSAVM00 model only.

Download firmware license file from a server and install it.

## syntax

upload\_license

Option	Description
-s	<server ip> Download an image file from this server IP address.
-t	[scp ftp] Type of download protocol. (Default= scp).
-u<username>	The user name for server authentication.
-p<password>	The password for server authentication.
-f<license filename>	The full path for the license file.

## hc-settings

Configure the unit as a HA-Cluster mode unit.

### syntax

hc-settings

Option	Description
-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.

Option	Description
-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.

### syntax

```
hc-status
```

Option	Description
-h	Help information.
-l	List the status of HA-Cluster units.

## hc-slave

Add/Update/Remove a slave unit to/from HA Cluster.

### syntax

```
hc-slave
```

## hc-master

Disable/Enable the malware detection features on master unit.

## syntax

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).

## cm-status

List the status of units joining the Global Threat Information Network

### syntax

`cm-status`

Option	Description
<code>-h</code>	Help information.
<code>-l</code>	List the status of units joining the Global Threat Information Network.

## 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`

Option	Description
<code>-a</code>	Add a confirmation ID.
<code>-c</code>	Confirmation ID.
<code>-d</code>	Delete a confirmation ID.
<code>-k</code>	License key.
<code>-l</code>	List all confirmation IDs.

## remote-auth-timeout

Set Radius or LDAP authentication timeout value.

### syntax

```
remote-auth-timeout
```

Option	Description
-h	Help information.
-s	Set timeout value to 10 to 180 seconds. (Default = 10).
-u	Unset timeout.
-l	Display timeout value.

## filesize-limit

Set file size limit of different input sources.

### syntax

```
filesize-limit
```

Option	Description
-h	Help information.
-l	Display the file size limitation.
-t [all ondemand netshare jsonrpc]	
-v [file size limitation (MBytes)]	(Range: 0 < size < 1024).

## log-dropped

Enable the log file drop event.

## syntax

log-dropped

Option	Description
-h	Help information.
-l	Show current config.
-e	Enable log dropped file.
-d	Disable log dropped file.

## reset-widgets

Reset your widgets.

### syntax

reset-widgets

## fortimail-expired

Enable/Disable expired timeout option for FortiMail files. By default, FortiMail will hold a mail for set period to wait for the verdict from FortiSandbox. When FSA scans an attachment or URL from FortiMail, it will check if the verdict is still needed as FortiMail might already have already released the email. If not, the scan will have an *Unknown* rating and skipped the status. Users can run this Option to enable or disable this expiration check.

### syntax

fortimail-expired

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

## raid-rebuild

Rebuild raid after a new HD replaces a bad one.

### syntax

```
raid-rebuild
```

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

## set-maintainer

Enable/disable maintainer account. Maintainer account is used to reset password of user admin

### syntax

```
set-maintainer
```

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

## set-tlsver

Set allowed TLS version for HTTPS service.

### syntax

```
set-tlsver
```



Option	Description
-h	Help information.
-l	Show current TLS versions.
-r	Reset to default versions
-e	Set allowed TLS versions. 1, 2 and 3 for TLS 1.0, 1.1 and 1.2 respectively. Separate versions with ' '. For example, -e1 2 3 to enable TLS 1.0, 1.1 and 1.2

## reset-sandbox-engine

Reset tracer and rating engines back to firmware default.

### syntax

```
reset-sandbox-engine
```

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.

# Utility Commands

## ping

Test network connectivity to another network host.

### syntax

```
ping <IP address>
```

## tcpdump

Examine local network traffic.

### syntax

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

Option	Description
-c	The tcpdump count.
-i	The tcpdump interface.
expression	The tcpdump expression.

## traceroute

Examine the route taken to another network host.

### syntax

```
traceroute <HOST>
```

## vm-customized

Install a new customized VM image.

## syntax

vm-customized

Option	Description
-h	Help information.
-c	Operation command.
n	
l	
f	
d	
-cn	Install a new customized VM.
-cl	List installed customized VM.
-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. (Default = 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 or meta file.
-k <MD5 checksum>	The MD5 checksum for uploaded vdi file.
-vo<OS type>	OS types: <ul style="list-style-type: none"> <li>• WindowsXP</li> <li>• Windows2003</li> <li>• Windows2008</li> <li>• Windows2008_64</li> <li>• Windows7</li> <li>• Windows7_64</li> <li>• Windows8</li> <li>• Windows8_64</li> <li>• Windows81</li> <li>• Windows81_64</li> <li>• Windows2012_64</li> <li>• Windows10</li> <li>• Windows10_64</li> </ul>

Option	Description
-vn<VM name>	The VM name.
-r<Replace VM if it exists>	Replace VM if it exists
-m<VM meta file name>	The VM meta filename.
-d	The machine UUID shown in the <code>.vbox</code> file on the image building host.

### example

To install a new customized image, and its meta data file, which contains installed applications 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/vdi_file_name> -vo<Windows_type> -vn<custom_vm_name> -k<MD5_in_lowercase_of_vdi_file> -d<MachineUUID>
```

```
vm-customized -cf -tftp -s<ftp_server_ip> -u<username> -p<password> -f</meta_file_path/meta_file_name> -vn<custom_vm_name> -mproduct.list
```

## reset-scan-profile

Reset clone # and file extension association of VM images to default values.

### syntax

```
reset-scan-profile
```

Option	Description
-h	Help information.
-l	Reset clone # and file extension association.

```
-h Help information.
-r Reset clone # and file extension association.
```

## sandboxing-prefilter

Allow user to turn on/off FortiGuard 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 FortiGuard 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 FortiGuard pre-filtering is enabled, only URLs whose web filtering rating is Unrated will be scanned inside associated guest VM image.

## syntax

sandboxing-prefilter

Option	Description
-h	Help information.
-e	Enable FortiGuard sandboxing prefilter.
-t	<p>Enable FortiGuard sandboxing prefilter for specific file types.</p> <ul style="list-style-type: none"> <li>• dll</li> <li>• pdf</li> <li>• swf</li> <li>• js</li> <li>• htm</li> <li>• url</li> <li>• office</li> <li>• trustvendor</li> </ul> <p>When <code>trustvendor</code> is selected, executable files from a small internal list of trusted vendors will skip the sandboxing scan step.</p>
-d	Disable FortiGuard sandboxing prefilter.
-t	<p>Disable sandboxing prefilter for specific file types.</p> <ul style="list-style-type: none"> <li>• dll</li> <li>• pdf</li> <li>• swf</li> <li>• js</li> <li>• htm</li> <li>• url</li> <li>• office</li> </ul>
-l	Display the status of FortiGuard 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.

## syntax

sandboxing-embeddedurl

Option	Description
-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 embedded URL.

# Diagnose Options

## 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]
               -cb|adapter_icap] [device_serial_number]
```

Option	Description
netshare	Network share daemon
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).
-cb	
adapter_icap	Daemon for Internet Content Adaptation Protocol (ICAP).
device_serial_number	The device serial number,

## diagnose-sys-top

Display current system top processes and current CPU/Memory usage.

### syntax

```
diag-sys-top
```

Option	Description
-h	Help information.
-l<value>	Maximum lines (Maximum = 100, default = 50).

Option	Description
-i<value>	Interval to delay in seconds (default = 5).
keyboard input operations:	
-q	or ^C Quit.
-m	Sort by Memory usage.
-p	Sort by CPU usage
-t	Sort by Time usage.
-n	Sort by PID

## diagnose-sys-perf

Display system performance information.

### syntax

diagnose-sys-perf

Option	Description
-h	Help information.
-m<value>	Last hours (maximum = 4 weeks (40320 hours), default = 1 hour).

### hardware-info

Display general hardware status information. Use this Option to view CPU, memory, disk, and RAID information, and system time settings.

### syntax

hardware-info

## disk-attributes

Display system disk attributes.

This CLI Option is available on hardware-based FortiSandbox models only.



**syntax**

disk-attributes

**disk-errors**

Display any system disk errors.

This CLI Option is available on hardware-based FortiSandbox models only.

**syntax**

disk-errors

**disk-health**

Display disk health information.

This CLI Option is available on hardware-based FortiSandbox models only.

**syntax**

disk-health

**disk-info**

Display disk hardware status information.

This CLI Option is available on hardware-based FortiSandbox models only.

**syntax**

disk-info

**raid-hwinfo**

Display RAID hardware status information.

This CLI Option is available on hardware-based FortiSandbox models only.

**syntax**

```
raid-hwinfo
```

**test-network**

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

**syntax**

```
test-network
```

# Glossary

## A

AAA  
Authentication, Authorization, and Accounting

AD  
Active Directory

ADOM  
Administrative Domain

AES  
Advanced Encryption Standard

AMI  
Amazon Machine Image

AP  
Access Point

API  
Application Programming Interface

APN  
Access Point Name

APT  
Advanced Persistent Threat

ATP  
Advanced Threat Protection

AV  
Antivirus

AVP  
Attribute Value Pairs

AWS  
Amazon Web Service

## B

BGP  
Border Gateway Protocol

## C

C&C  
Option and Control

- CA  
Certificate Authority
- CASI  
Cloud Access Security Inspection
- CBC  
Cipher Block Chaining
- CHAP  
Challenge-Handshake Authentication Protocol
- CIDR  
Classless Inter-Domain Routing
- CLI  
Option Line Interface
- CN  
Common Name
- CoA  
Change of Authorization
- CPU  
Central Processing Unit
- CRL  
Certificate Revocation List
- CSR  
Certificate Signing Request
- CSV  
Comma Separated Value
- CVE  
Common Vulnerabilities and Exposures

**D**

- DC  
Domain Controller, Direct Current
- DES  
Data Encryption Standard
- DH  
Diffie-Hellman
- DHCP  
Dynamic Host Configuration Protocol
- DLL  
Dynamic-Link Library

DLP  
Data Loss Prevention

DN  
Distinguished Name

DNAT  
Destination Network Address Translation

DNS  
Domain Name System

DSCP  
Differentiated Services Code Point

DSRI  
Disable Server Response Inspection

DTLS  
Datagram Transport Layer Security

## E

EA  
E-mail Address

EAPOL  
Extensible Authentication Protocol over LAN (Local Area Network)

EC  
Endpoint Control

EC2  
Elastic Compute Cloud

EGP  
Exterior Gateway Protocol

EMS  
Enterprise Management Server

ESD  
Electrostatic Discharge

ESP  
Encapsulated Security Payload

## F

FAZ  
FortiAnalyzer

FCT  
FortiClient

FDN  
FortiGuard Distribution Network

FDS  
FortiGuard Distribution Servers

FG  
FortiGate

FGFM  
FortiGate-FortiManager

FMG  
FortiManager

FQDN  
Fully Qualified Domain Name

FSA  
FortiSandbox

FSSO  
Fortinet Single Sign-On

FTP  
File Transfer Protocol

## G

GCF  
Gatekeeper Confirm

GPRS  
General Packet Radio Service

GRE  
Generic Routing Encapsulation

GTP  
GPRS Tunneling Protocol

GUI  
Graphical User Interface

GUID  
Globally Unique Identifier

## H

HA  
High Availability

hcache  
Hard Cache

HDD  
Hard Disk Drive

HTML  
HyperText Markup Language

HTTP  
HyperText Transfer Protocol

## I

I/O  
Input / Output

IBP  
Identity-based Policy

ICAP  
Internet Content Adaptation Protocol

ICMP  
Internet Control Message Protocol

IGP  
Interior Gateway Protocol

IKE  
Internet Key Exchange

IMAP  
Internet Message Access Protocol

IOC  
Indicators of Compromise

IP  
Internet Protocol

IPS  
Intrusion Prevention System

IPsec  
Internet Protocol Security

ISDB  
Internet Service Database

ISP  
Internet Service Provider

IV  
Initialization Vector

## J

JSON  
JavaScript Object Notation

## L

L2TP  
Layer 2 Tunneling Protocol

LACP  
Link Aggregation Control Protocol

LAN  
Local Area Network

LDAP  
Lightweight Directory Access Protocol

## M

MAC  
Media Access Control

MD5  
Message Digest 5

MGCP  
Media Gateway Controller Protocol

MIB  
Management Information Base

MMC  
Microsoft Management Console

MSCHAP  
Microsoft Challenge-Handshake Authentication Protocol

MSS  
Maximum Segment Size

## N

NAC  
Network Access Control or Compliance

NAS  
Network Access Server

NAT  
Network Address Translation

NAT-PT  
Network Address Translation (NAT) Port Translation

NDcPP  
Network Device Collaborative Protection Profile

NGFW  
Next-Generation Firewall

NNTP  
Network News Transfer Protocol

NOC  
Network Operations Center



NPU  
Network Processing Unit

NTLM  
NT LAN Manager

NTP  
Network Time Protocol

## O

OCSP  
Online Certificate Status Protocol

OFTP  
Odette File Transfer Protocol

ONC-RPC  
Open Network Computing Remote Procedure Call

OSPF  
Open Shortest Path First

OTP  
One-time Password

OU  
Organization Unit

OUI  
Organizationally Unique Identifier

OVF  
Open Virtualization Format

## P

PAP  
Password Authentication Protocol

PAT  
Port Address Translation

PEM  
Power Entry Module

PFS  
Perfect Forward Secrecy

PKCS  
Public Key Cryptography Standards

PKI  
Public Key Infrastructure

PoE  
Power over Ethernet

POP3  
Post Office Protocol 3

PPP  
Point-to-Point Protocol

PPPoE  
Point-to-Point Protocol over Ethernet

PPTP  
Point-to-Point Tunneling Protocol

PSK  
Pre-Shared Key

## R

RADIUS  
Remote Authentication Dial-In User

RAID  
Redundant Array of Independent Disks

RAM  
Random Access Memory

RAS  
Registration, Admission, and Status

RBAC  
Role Based Access Control

RCF  
Registration Confirm

RDP  
Remote Desktop Protocol

REST  
Representational State Transfer

RFC  
Remote Function Call

RSH  
Remote Shell

RSSO  
RADIUS Single Sign-On

RTM  
Real-Time Monitor

RTP  
Real-Time Protection

RTSP  
Real-Time Streaming Protocol

## S

SAN  
Storage Area Network

SAP  
Shelf Alarm Panel

SCEP  
Simple Certificate Enrollment Protocol

SCP  
Secure Copy

SCVP  
Server-based Certificate Validation Protocol

SDK  
Software Development Kit

SDN  
Software-Defined Networking

SFTP  
Secure (or SSH) File Transfer Protocol

SHA1  
Secure Hash Algorithm 1

SIP  
Session Initiation Protocol

SMTP  
Simple Mail Transfer Protocol

SNAT  
Secure Network Address Translation

SNI  
Server Name Indication

SNMP  
Simple Network Management Protocol

SOC  
Security Operations Center

SQL  
Structured Query Language

SSH  
Secure Shell

SSID  
Service Set Identifier

SSL  
Secure Sockets Layer

SSO  
Single Sign-On

## T

TACACS+  
Terminal Access Controller Access-Control System

Tcl  
Tool Option Language

TCP  
Transmission Control Protocol

TFTP  
Trivial File Transfer Protocol

TLS  
Transport Layer Security

TNS  
Transparent Network Substrate

TTL  
Time-to-live

## U

UDP  
User Datagram Protocol

UID  
Unique Identifier

URI  
Uniform Resource Identifier

URL  
Uniform Resource Locator

UTM  
Unified Threat Management

UUID  
Universally Unique Identifier

## V

VDOM  
Virtual Domain

VHD  
Virtual Hard Disk

VIP  
Virtual Internet Protocol

VLAN  
Virtual Local Area Network

VM  
Virtual Machine

VMDK  
Virtual Machine Disk

VoIP  
Voice over Internet Protocol

VPC  
Virtual Private Cloud

VPN  
Virtual Private Network

VSA  
Vendor Specific Attribute

## W

WAF  
Web Application Firewall

WAN  
Wide Area Network

WCCP  
Web Cache Communication Protocol

WIDS  
Wireless Intrusion Detection System

WPA  
Wi-Fi Protected Access

WPA2  
Wi-Fi Protected Access II

WSDL  
Web Services Description Language

WTP  
Wireless Transaction Protocol

## X

XAuth  
Extended Authentication

XML  
eXtensible Markup Language

XSS  
Cross-site Scripting

XVA  
XenServer Virtual Appliance

# Index

## C

CLI 6-7, 32

CPU 31

## F

firmware 11

## I

IP address 8, 13, 26

## L

license 15

file 18

## M

MAC 8

Media Access Control See MAC

## O

Option Line Interface See CLI

## P

password 13, 27

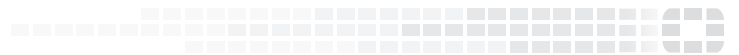
## S

Secure Shell See SSH

SSH 6



**FORTINET®**



Copyright© 2018 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.