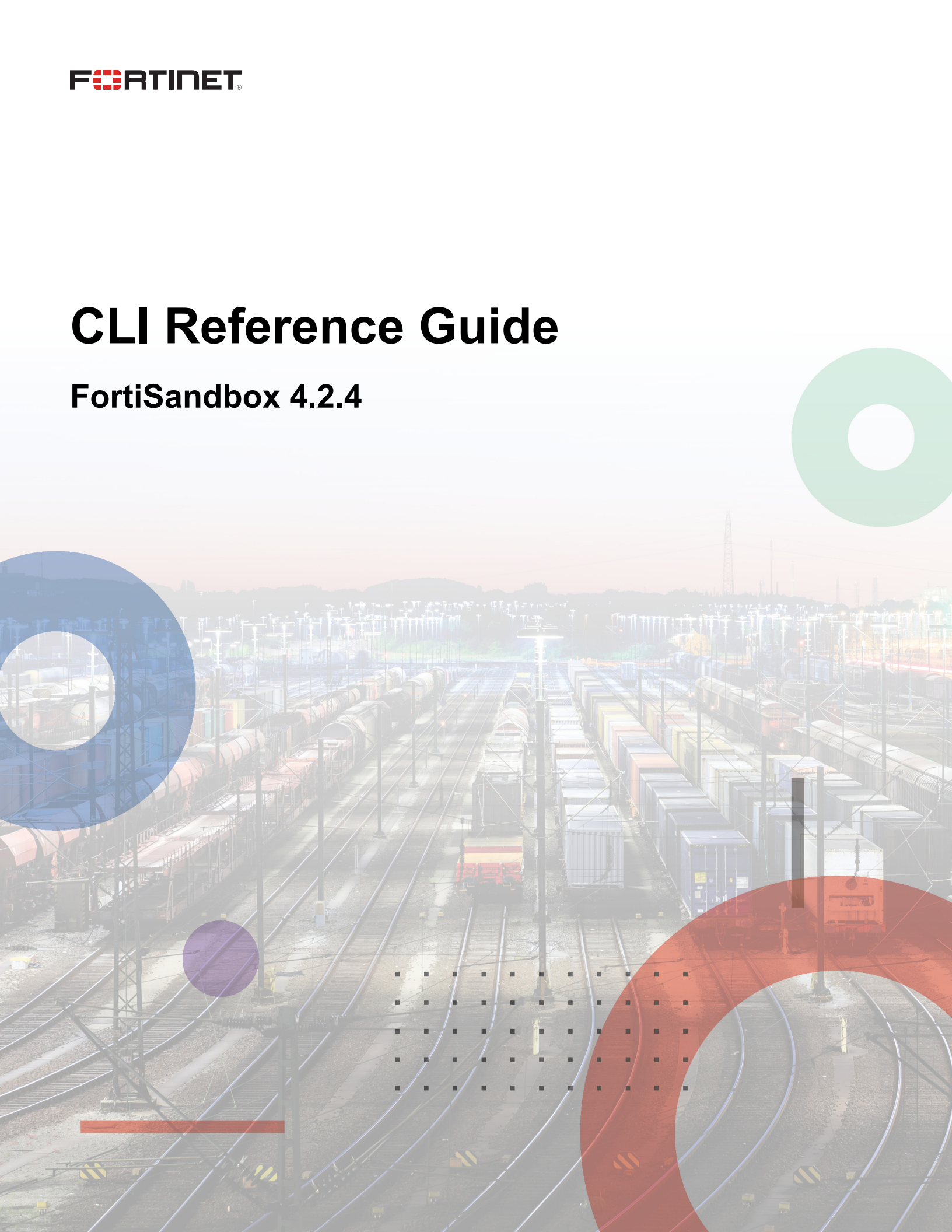


CLI Reference Guide

FortiSandbox 4.2.4



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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 CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



July 17, 2023

FortiSandbox 4.2.4 CLI Reference Guide

34-424-881335-20230717

TABLE OF CONTENTS

Introduction	5
Configuration commands	6
System commands	7
ai-mode	10
backup-sysconf	11
confirm-id	11
device-authorization	12
device-clean-pdf	13
device-lenc	13
filesize-limit	14
fortimail-expired	14
fw-upgrade	15
hc-primary	15
hc-settings	16
hc-status	17
hc-worker	17
inline-block-timeout	18
iptables	18
log-dropped	20
oftpd-con-mode	20
pending-jobs	20
prescan-config	22
processing-jobs	22
raid-rebuild	23
remote-auth-timeout	23
reset-sandbox-engine	24
reset-scan-profile	24
restore-sysconf	25
sandboxing-adaptive	25
sandboxing-cache	25
sandboxing-embeddedurl	26
sandboxing-parallel	26
sandboxing-pexbox	27
sandboxing-pipeline	27
sandboxing-prefilter	28
sandboxing-ratio	29
sandboxing-rse	29
set-cfg-backup-key	29
set-maintainer	30
set-tcp-timestamp-response	30
set-tlsver	31

upload-license	31
upload-settings	32
url-recheck	32
usg-license	33
vm-customized	33
vm-internet	34
vm-license	34
vm-reset	35
Utility commands	36
Diagnose commands	37
diagnose-clilog	38
diagnose-debug	38
diagnose-kernlog	38
diagnose-sys-top	39
test-network	40
Change log	41

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.

Configuration commands

The following configuration commands are available:

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 a sniffer, it will not be displayed.
set	<div>Set configuration parameters.</div> <div><div>set admin-port <portx></div><div>Enable a new administrative port other than port1. It cannot be set to port3 or sniffer ports.</div></div> <div><div>set api-port</div><div>Set ports for API connection.</div></div> <div><div>set date <date></div><div>Set system date, in the format of YYYY-MM-DD.</div></div> <div><div>set default-gw <ip></div><div>Set the default gateway address.</div></div> <div><div>set port3-speed [<auto> <speed full half>]</div><div>Set port3 speed and duplex settings. The option port3-speed is not for FSA_VM.</div></div> <div><div>set port-mtu <portx> <1200-9000></div><div>Set a port's MTU value.</div></div> <div><div>set portX-ip <ip/netmask></div><div>Set the portX IP address in IP/netmask format. It can also set the address on aggregate ports.</div></div> <div><div>set time <time></div><div>Set system time, in the format of HH:MM:SS.</div></div>
unset	<div>Unset the admin port or the default gateway:</div> <div><ul style="list-style-type: none">unset admin-portunset api-portunset default-gw</div>

System commands

Command	Description
ai-mode	Enable/disable using AI logic to do job's behavior analysis. For details, see ai-mode on page 10 .
backup-sysconf	Upload system configuration backup to remote server. For details, see backup-sysconf on page 11 .
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 <i>Scan Profile</i> settings are set back to default.
confirm-id	Set confirm ID for Microsoft Windows or Office activation. For details, see confirm-id on page 11 .
device-authorization	Configure new client device authorization . For details, see device-authorization on page 12 .
device-lenc	Enable/disable OFTPD supporting FortiGate-LENC devices. For details, see device-lenc on page 13 .
device-clean-pdf	FortiSandbox will send job detail PDF to FortiGate when requested. For details, see device-clean-pdf on page 13 .
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 <i>Scan Profile</i> settings are set back to default.
filesize-limit	Set the maximum single file size and the maximum child file size to scan. For details, see filesize-limit on page 14 .
fortimail-expired	Enable/disable expired timeout option for FortiMail files. For details, see fortimail-expired on page 14 .
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. For details, see fw-upgrade on page 15 .
hc-primary	Enable/disable the malware detection features on the primary unit.

Command	Description
	Use <code>-s<percent></code> to turn on file scan and set the percentage of the scanning capacity to be used. If no number is entered, 50% will be used. For details, see hc-primary on page 15
<code>hc-settings</code>	Configure the unit as a HA-Cluster mode unit. For details, see hc-settings on page 16 .
<code>hc-status</code>	List the status of HA-Cluster units. For details, see hc-status on page 17 .
<code>hc-worker</code>	Add/update/remove a worker unit to/from an HA-Cluster. This command can only be run on a worker unit. For details, see hc-worker on page 17 .
<code>inline-block-timeout</code>	Set the timeout value to replay the request from FortiOS. For details, see inline-block-timeout on page 18 .
<code>iptables</code>	Enable/disable IP tables. For details, see iptables on page 18 .
<code>log-dropped</code>	Enable/disable the log file drop event. For details, see log-dropped on page 20 .
<code>log-purge</code>	Delete all system logs.
<code>oftpd-con-mode</code>	Enable/disable conserve mode of OFTPD. For details, see oftpd-con-mode on page 20 .
<code>pending-jobs</code>	Show the status of or delete pending jobs. For details, see pending-jobs on page 20 .
<code>prescan-config</code>	Configure support for large files of up to 10GB in VM. For details, see prescan-config on page 22 .
<code>raid-rebuild</code>	Rebuild raid after a new HD replaces a bad one. This option is only available on hardware models. For details, see raid-rebuild on page 23 .
<code>reboot</code>	Reboot the FortiSandbox. All sessions will be terminated. The unit goes offline and there is a delay while it restarts.
<code>remote-auth-timeout</code>	Set the timeout for remote authentication. For details, see remote-auth-timeout on page 23 .
<code>reset-sandbox-engine</code>	Reset the tracer/rating engine back to firmware default. For details, see reset-sandbox-engine on page 24 .
<code>reset-scan-profile</code>	Reset the scan flow settings to firmware default values. For details, see reset-scan-profile on page 24 .
<code>reset-widgets</code>	Reset the GUI widgets.

Command	Description
<code>resize-hd</code>	After changing the virtual hard disk size on the hypervisor, execute this command to make the change recognizable to the firmware. This command is only available for FSA_VM-Base and FSAVM00 models.
<code>restore-sysconf</code>	Restore system configuration from remote server. For details, see restore-sysconf on page 25 .
<code>sandbox-engines</code>	Display FortiSandbox FortiGuard component versions including the Tracer Engine, Rating Engine, Traffic Sniffer, Botnet Signature Database, IPS Signature Database, and Android engine versions.
<code>sandboxing-adaptive</code>	Enable/disable adaptive scan. For details, see sandboxing-adaptive on page 25 .
<code>sandboxing-cache</code>	Enable/disable sandboxing result check. For details, see sandboxing-cache on page 25 .
<code>sandboxing-embeddedurl</code>	Enable/disable sandboxing embedded urls in PDF or OFFICE documents. For details, see sandboxing-embeddedurl on page 26 .
<code>sandboxing-parallel</code>	Enable/disable parallel scan. For details, see sandboxing-parallel on page 26 .
<code>sandboxing-pexbox</code>	Turn the PE emulator on or off. For details, see sandboxing-pexbox on page 27 .
<code>sandboxing-pipeline</code>	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. For details, see sandboxing-pipeline on page 27 .
<code>sandboxing-prefilter</code>	Enable/disable sandboxing prefilter for file types. For details, see sandboxing-prefilter on page 28 .
<code>sandboxing-ratio</code>	Set VM scan ratio. For details, see sandboxing-ratio on page 29 .
<code>sandboxing-rse</code>	Enable/disable/view Rating Service Endpoint API. For details, see sandboxing-rse on page 29 .
<code>set-cfg-backup-key</code>	Set your own passphrase that openssl uses to encrypt or decrypt a configuration backup file. For details, see set-cfg-backup-key on page 29 .
<code>set-maintainer</code>	Enable/disable the maintainer account. For details, see set-maintainer on page 30 .
<code>set-tlsver</code>	Set the allowed TLS version for HTTPS service. For details, see set-tlsver on page 31 .
<code>shutdown</code>	Shutdown the FortiSandbox.

Command	Description
<code>status</code>	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.
<code>upload-settings</code>	Configure data upload settings to community cloud. For details, see upload-settings on page 32 .
<code>url-recheck</code>	Enable/disable trusting previous scan results in Fortimail URL scan. For details, see url-recheck on page 32 .
<code>usg-license</code>	Convert the unit to be USG licensed. For details, see usg-license on page 33 .
<code>vm-customized</code>	Install customized VM. For details, see vm-customized on page 33 .
<code>vm-internet</code>	Allow Virtual Machines to access external network through outgoing port3 and set gateway for port3. For details, see vm-internet on page 34 .
<code>vm-license</code>	List embedded Windows Product key information. For details, see vm-license on page 34 .
<code>vm-reset</code>	Activate and initialize a VM image again, in case it is necessary to rebuild a VM image. Optionally, specify a VM name with <code>-n <VM name></code> , or all VMs are reset. For details, see vm-reset on page 35 .
<code>vm-status</code>	Show VM system status and their license situation. If there is an issue with a VM, an error message displays information to help troubleshoot the problem.

ai-mode

Enable/disable using AI logic to do job's behavior analysis (default).

In cluster mode, this setting is synchronized to all the nodes. It can be set on standalone or primary units.

This command can only be run by users whose profile has *Scan Policy* enabled.

Syntax

```
ai-mode <option>
```

Option	Description
<code>-h</code>	Help information.
<code>-l</code>	Display the current AI mode setting.

Option	Description
-e	Enable using AI logic to do job's behavior analysis (default).
-d	Disable using AI logic to do job's behavior analysis.

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
```

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> [options]
```

Option	Description
-a	Add a confirmation ID
-k	License key.
-c	Conformation ID.
-n	Name of VM.

Option	Description
-d	Delete a confirmation ID.
-k	License key.
-l	List all confirmation IDs.

Example

To 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 <option>
```

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
```

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

device-clean-pdf

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

Syntax

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

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

device-lenc

Enable/disable OFTPD supporting FG-LENC devices.

Syntax

```
device-lenc <option>
```

Option	Description
-h	Help information.
-e	Enable support for Low-Encryption (LENC) devices.
-d	Disable support for Low-Encryption (LENC) devices (default).
-l	Display current support status for Low-Encryption (LENC) devices.

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: 200MB
- Uncompressed Size: 500MB



The maximum file size allowed for a device is 512MB.

Syntax

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

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



The upper bound for FSA_VM on demand is 10240MB.

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.

fw-upgrade

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

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

Syntax

```
fw-upgrade <option> [options]
```

Option	Description
-h	Help information.
-b	Download an image file from this server and upgrade the firmware.
-v	Download a VM image file from this server and install.
-t<ftp https scp>	The protocol type, FTP, HTTPS, or SCP (default = SCP).
-s<IP address>	The IP address of the server that the image will be downloaded from.
-u<user name>	The user name for authentication.
-f<file path>	The full path for the image file.

Example

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

hc-primary

Configure the unit as a HA-Cluster primary unit.

syntax

```
hc-primary [-h|-u|-s|-l|-r]
```

Option	Description
-h	Help information.
-u	Turn off file scan on primary unit.
-s<10-100>	Turn on file scan on primary unit with 10% to 100% processing capacity.
-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 <option> [options]
```

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	Primary unit.
P	Secondary unit.
R	Worker unit.
-n<name string>	Set alias name for this unit.
-c<HA-CLUSTER name>	Set the HA-Cluster name for primary unit.
-p<authentication code>	Set the authentication code for primary unit.
-i<interface>	Set interface used for cluster internal communication.
-si	Set the fail-over IPs for this cluster for primary unit.
-i<interface>	Specify the interface for external communication
-a<IP/netmask>	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.
-se	Enable traffic encryption between HA cluster members.
-sd	Disable traffic encryption between HA cluster members.

Example

To create a primary node:

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

hc-status

Check HA-Cluster status.

syntax

```
hc-status <option> [options]
```

Option	Description
-h	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 <option>
```

Option	Description
-h	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 -10.0.2.5 -p1111
```

inline-block-timeout

Set the timeout value to replay the request from FortiOS.

Syntax

```
inline-block-timeout <option>
```

Option	Description
-a<skip/scan>	Set action of timeout file.
-h	Help information.
-l	Display the current settings.
-r	Revert to the default value.
-s<seconds>	Set timeout value

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.

--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).

<code>--replace -R chain rulenum</code>	Replace rule rulenum (1 = first) in chain.
<code>--list -L [chain [rulenum]]</code>	List the rules in a chain or all chains.
<code>--list-rules -S [chain [rulenum]]</code>	Print the rules in a chain or all chains.
<code>--flush -F [chain]</code>	Delete all rules in chain or all chains.
<code>--zero -Z [chain [rulenum]]</code>	Zero counters in chain or all chains.
<code>--new -N chain</code>	Create a new user-defined chain.
<code>--delete-chain -X [chain]</code>	Delete a user-defined chain.
<code>--policy -P chain target</code>	Change policy on chain to target.
<code>--rename-chain -E old-chain new-chain</code>	Change chain name, (moving any references).

Options

Either long or short options are allowed.

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

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.

pending-jobs

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

Syntax

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

Option	Description
-h	Help information.
show / purge	Show or purge the pending jobs.
source	One of: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • all - All job queues. • vm - Sandboxing job queue. • nonvm - non-Sandboxing job queue. • pre - Files pending to enter job queue.
filetype	One of: <ul style="list-style-type: none"> • 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.

Syntax

```
prescan-config [-h|-l|-c|-n|-b|-u]
```

Option	Description
-h	Help information.
-l	Show prescan settings.
-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.
-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.
-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.
-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 list IDs of processing jobs.
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
```

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.

remote-auth-timeout

Set Radius or LDAP authentication timeout value.

Syntax

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

Option	Description
-h	Help information.

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

reset-sandbox-engine

Reset tracer and rating engines back to firmware default.

Syntax

```
reset-sandbox-engine <option>
```

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* > *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.

Syntax

```
reset-scan-profile [-r|-h]
```

Option	Description
-h	Help information.
-r	Reset the VM profile to be default.

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
```

sandboxing-adaptive

Turn adaptive scan on or off.

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-cache

Turn the sandboxing result cache on or off.

When it is off, the same file will be scanned again by sandboxing. When it is on, sandboxing scan results will be added to an internal cache and reused in future when the same file is scanned.

When the scan condition is changed, such as when a new tracer engine is installed, the cache will be purged.

Syntax

```
sandboxing-cache <option>
```

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

sandboxing-embeddedurl

Turn on or off sandboxing embedded URLs in PDF or Office documents. Only randomly selected URLs will be scanned.

Syntax

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

Option	Description
-h	Help information.
-e	Enable sandboxing embedded URLs in PDF or Office documents.
-d	Disable status for sandboxing embedded URLs (default).
-i	Disable embedded URL extraction in PDF or Office documents.
-l	Display the status of sandboxing embedded URL.

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-pexbox

Turn PE emulator on or off.

Syntax

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

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

sandboxing-pipeline

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

Syntax

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

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

sandboxing-prefilter

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

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

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

Syntax

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

Option	Description
-h	Help information.
-e	Enable sandboxing prefilter. <ul style="list-style-type: none"> -t [dll pdf swf js htm url office trustvendor trustdomain archive trustfndr]: Enable sandboxing prefilter for specific types.
-d	Disable sandboxing prefilter. <ul style="list-style-type: none"> -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	<p>Enable/disable sandboxing prefilter for specific file types: archive, dll, pdf, swf, js, htm, url, office, trustvendor, trustdomain, trustfndr.</p> <p>archive and trustdomain are enabled by default. Other prefilters are disabled by default.</p> <p>When trustvendor is selected, executable files from a small internal list of trusted vendors will skip the sandboxing scan step.</p> <p>When trustdomain is selected, files downloaded from a small internal list of trusted domains will skip the sandboxing scan step.</p> <p>When trustfndr is selected, files rated by FortiNDR as clean or malicious will skip the sandboxing VM scan step.</p>
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.

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 <option>
```

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.

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 <option>
```

Option	Description
-h	Help information.
-e	Enable the specified upload setting.
-d	Disable the specified upload setting.
-t[uploadcloud submiturl uploadstats]	Set the type of upload setting: <ul style="list-style-type: none">• uploadcloud: Upload malicious and suspicious file information to Sandbox Community Cloud. Default is enabled.• submiturl: Submit suspicious URL to Fortinet WebFilter service. Default is disabled.• uploadstats: Upload statistics data to FortiGuard service. Default is disabled.
-l	Display the status of the upload settings

Example

To enable upload statistics to FortiGuard services:

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

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
-l	Display the status of this setting.

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.

vm-customized

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

Syntax

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

Option	Description
-h	Help information.
-c[n l f d u]	Operation command.
n	Install a new customized VM.
l	List installed customized VM.
f	Upload a meta file for a customized VM.
d	Display a meta file for a customized VM.
u	Upload a VDI file to a remote server. Supported protocols include TFTP, FTP, and SCP.
-t<ftp scp tftp>	The protocol type, FTP, SCP (default) or tftp.
-s<server IP>	Download the image file from this FTP or SCP server IP address.
-u<user name>	User name for authentication.

Option	Description
-f<full path of filename>	Full path for the image file or meta file.
-d<hardware/machine ID>	Original hardware ID or machine ID.
-k<MD5 checksum>	MD5 checksum for the uploaded file.
-v[o n]	Set the base information for VM image
o<OS type>	WindowsXP, Windows7, Windows7_64, Windows81, Windows81_64 , Windows10, or Windows10_64.
n<VM name>	Name of the VM.
-r <VM name>	Replace the VM if it already exists.
-m <VM meta file name>	Name of the VM meta file.

vm-internet

Syntax

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

Option	Description
-h	Help information.
-l	Display the current configuration.
-s	Set the 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.

vm-license

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

Syntax

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

Option	Description
-h	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.

Utility commands

The following utilities are available.

Command	Description
ping	Test network connectivity to another network host: <code>ping <IP address> [-c count -vb default -c0 continuous ping]</code>
tcpdump	Examine local network traffic: <code>tcpdump [-c count] [-i interface] [expression]</code>
tracert	Examine the route taken to another network host: <code>tracert <host></code>

Diagnose commands

The following diagnostic commands are available:

Command	Description
<code>diagnose-cliilog</code>	Record all CLI input and output. See diagnose-cliilog on page 38 for details.
<code>diagnose-debug</code>	Display detailed debug logs of network share scan and communications with devices. See diagnose-debug on page 38 for details.
<code>diagnose-krnlog</code>	Record the kernel ring buffer. See diagnose-krnlog on page 38 for details.
<code>diagnose-sys-perf</code>	Display system performance information. Optionally, specify how many previous hours to show with <code>-m<hours></code> (maximum = 40320, default = 1).
<code>diagnose-sys-top</code>	Display system top information. See diagnose-sys-top on page 39 for details.
<code>disk-attributes</code>	Display system disk attributes. This option is only available on hardware models.
<code>disk-errors</code>	Display any system disk errors. This option is only available on hardware models.
<code>disk-health</code>	Display disk health information. This option is only available on hardware models.
<code>disk-info</code>	Display disk hardware status information. This option is only available on hardware models.
<code>hardware-info</code>	Display general hardware status information. Use this option to view CPU, memory, disk, and RAID information, as well as system time settings.
<code>raid-hwinfo</code>	Display RAID hardware status information, including if auto RAID (AutoRebuild) is enabled. This option is only available on hardware models.
<code>tac-report</code>	A collection of config, diagnose, system, and utility commands for monitoring and troubleshooting purposes.
<code>test-network</code>	Test the network connection. Use the output to detect network speed and connection to FDN servers and Microsoft servers. For details, see test-network on page 40 .

diagnose-clilog

Record and display CLI inputs and outputs.

Syntax

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

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

diagnose-debug

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

Syntax

```
diagnose-debug [netshare|device|adapter] [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).
adapter_bcc	Daemon for BCC.
adapter_mta_relay	Daemon for MTA relay.
device_serial_number	The device serial number.

diagnose-krnlog

Record and display kernel logs.

Syntax

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

Option	Description
-h	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-top

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

Syntax

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

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

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 type help)	Help information.
local_resolve_speed	Test system DNS resolve.
ping_speed	Test ping speed.
wget_speed	Test wget speed.
fdn	Test FDN service.
web_filter	Test Web Filtering service.
cloud	Test FSA community cloud service.
cloudvm	Test FSA Dynamic Scan (Cloud) VM service.
vm_connect	Test VM Internet access via port3.
connect	Test system Internet connection.
resolve_speed	Test VM DNS resolve speed.
vm_downloadable	Test VM downloadable.
rating_service_endpoint	Test Cloud rating.
sandbox_community_upload	Test sandbox community cloud submission status.
webfilter_upload	Test webfilter service submission status.
fortiguard_upload	Test statistics data submission to Fortiguard service status.
fndr_connection	Test FortiNDR service.
faz_connection	Test FortiAnalyzer server connection.
aws	Test AWS config connection (FortiSandbox on AWS only).
azure	Test Azure config connection (FortiSandbox on Azure only)

Change log

Date	Change Description
2023-03-01	Initial release.
2023-04-21	Added upload-license on page 31.
2023-04-24	Updated set-tcp-timestamp-response on page 30.
2023-04-25	Updated processing-jobs on page 22.
2023-07-17	Updated diagnose-sys-top on page 39, Utility commands on page 36, hc-worker on page 17, oftpd-con-mode on page 20, raid-rebuild on page 23 and remote-auth-timeout on page 23.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.