FortiSandbox - CLI Reference Guide

Version 3.1.3

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

June 09, 2020
FortiSandbox 3.1.3 CLI Reference Guide
34-313-631797-20200609

TABLE OF CONTENTS

Introduction 4
What's New in FortiSandbox 5
Configuration Commands 6
System Commands 7
fw-upgrade 9
pending-jobs 10
device-authorization 11
iptables 12
usg-license 13
hc-settings 14
hc-slave 15
hc-master 15
hc-status 16
confirm-id 16
vm-customized 16
sandboxing-cache 17
sandboxing-prefilter 18
sandboxing-embeddedurl 18
filesize-limit 19
remote-auth-timeout 19
log-dropped 20
vm-internet 20
raid-rebuild 21
reset-sandbox-engine 21
set-maintainer 21
set-tcp-timestamp-response 22
set-tlsver 22
fortimail-expired 23
oftpd-con-mode 23
device-lenc 24
upload-settings 24
ai-mode 25
Utility Commands 26
Diagnose Commands 27
diagnose-clilog 27
diagnose-krnlog 28
diagnose-debug 28
diagnose-sys-top 29
Change Log 30

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.

What’s New in FortiSandbox

The following tables list the commands and variables that have changed in version 3.1.3.

Command	Description
`ping`	This command now supports continuous ping. `ping <IP address> [ -c count | -vb default | -c0 continuous ping]`
`fw-upgrade`	This command now supports HTTPS option.
`set-tcp-timestamp-response`	New command to enable or disable TCP timestamp response.

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`	Set configuration parameters. • `set portX-ip <ip/netmask>` - Set the portX IP address in IP/netmask format. • `set port3-speed [<auto> | <speed full | half>]` - Set port3 speed and duplex settings. The option `port3-speed` is not for FSA_VM. • `set port-mtu <portx> <1200-9000>` - Set a port's MTU value. • `set admin-port <portx>` - Enable a new administrative port other than port1. It cannot be set to port3 or sniffer ports. • `set default-gw <ip>` - Set the default gateway address. • `set date <date>` - Set system date, in the format of YYYY-MM-DD. • `set time <time>` - Set system time, in the format of HH:MM:SS.
`unset`	Unset the admin port or the default gateway: • `unset admin-port` • `unset default-gw`

System Commands

Command	Description
`reboot`	Reboot the FortiSandbox. All sessions will be terminated. The unit will go offline and there will be a delay while it restarts.
`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.
`factory-reset`	Reset the FortiSandbox configuration to factory default settings. All data are deleted. For installed VM images, only Default VMs are kept and their clone number and *Scan Profile* settings are set to default values.
`shutdown`	Shutdown the FortiSandbox.
`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.
`sandbox-engines`	Display FortiSandbox FortiGuard component versions including the Tracer Engine, Rating Engine, Traffic Sniffer, Botnet Signature Database, IPS Signature Database, and Android engine versions.
`vm-license -l`	List embedded Windows Product key information.
`vm-status`	Show VM system status and their license situation. If there is an issue with a VM, an error message will be displayed with information to help troubleshoot the problem.
`vm-reset`	Activate and initialize a VM image again. Sometimes it is necessary to rebuild a VM image when it is broken. Optionally, specify a VM name with `-n <VM name>`, or all VMs will be reset.
`fw-upgrade`	Upgrade or re-install the FortiSandbox firmware via Secure Copy (SCP) or File Transfer Protocol (FTP) server. See fw-upgrade on page 9 for details.
`reset-widgets`	Reset the GUI widgets.
`cleandb`	Clean up the internal database and job information. This command will erase all stored data and reboot the device. This command only works on devices that are in standalone mode.
`pending-jobs`	Show the status of or delete pending jobs. See pending-jobs on page 10 for details.
`device-authorization`	Configure new client device authorization . See device-authorization on page 11 for details.

Command	Description
`log-purge`	Delete all system logs.
`iptables`	Enable/disable IP tables. See iptables on page 12 for details.
`usg-license`	Convert the unit to be USG licensed. See usg-license on page 13 for details.
`hc-settings`	Configure the unit as a HA-Cluster mode unit. See hc-settings on page 14 for details.
`hc-status`	List the status of HA-Cluster units.
`hc-slave`	Add/update/remove a slave unit to/from an HA-Cluster. This command can only be run on a slave unit.
`hc-master`	Enable/disable the malware detection features on master unit. Use `-s<percent>` 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.
`resize-hd`	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.
`confirm-id`	Set confirm ID for Microsoft Windows or Office activation. See confirm-id on page 16 for details.
`vm-customized`	Install customized VM. See vm-customized on page 16 for details.
`sandboxing-cache`	Enable/disable sandboxing result check. See sandboxing-cache on page 17 for details.
`reset-scan-profile`	Reset the clone number and file extension association back to firmware default values using the `-r` option.
`sandboxing-prefilter`	Enable/disable sandboxing prefilter for file types. See sandboxing-prefilter on page 18 for details.
`sandboxing-embeddedurl`	Enable/disable feature for sandboxing embedded urls in PDF or OFFICE documents. See sandboxing-embeddedurl on page 18 for details.
`filesize-limit`	Set file size limitation for scan input type, in megabytes (default = 200). See filesize-limit on page 19 for details.
`remote-auth-timeout`	Set the timeout for remote authentication. See remote-auth-timeout on page 19 for details.
`cm-status -l`	List the status of units joining the Global Threat Information Network.
`log-dropped`	Enable/disable the log file drop event. See log-dropped on page 20 for details.

Command	Description
`vm-internet`	Allow Virtual Machines to access external network through outgoing port3 and set gateway for port3. See vm-internet on page 20 for details.
`fsck-storage`	Check the file system on the hard disk and repair it if it's not clean. System reboots immediately.
`raid-rebuild`	Rebuild raid after a new HD replaces a bad one. See raid-rebuild on page 21 for details.
`reset-sandbox-engine`	Reset the tracer/rating engine back to firmware default. See reset-sandbox-engine on page 21 for details.
`set-maintainer`	Enable/disable the maintainer account. See set-maintainer on page 21 for details.
`set-tlsver`	Set the allowed TLS version for HTTPS service. See set-tlsver on page 22 for details.
`fortimail-expired`	Enable/disable expired timeout option for FortiMail files. See fortimail-expired on page 23 for details.
`oftpd-con-mode`	Enable/disable conserve mode of OFTPD. See oftpd-con-mode on page 23 for details.
`device-lenc`	Enable/disable OFTPD supporting FortiGate-LENC devices. See device-lenc on page 24 for details.
`upload-settings`	Configure data upload settings to community cloud. See upload-settings on page 24 for details.
`ai-mode`	Enable/disable using AI logic to do job's behavior analysis. See ai-mode on page 25 for details.

fw-upgrade

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

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.

pending-jobs

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

Syntax

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

Option	Description
`show / purge`	Show or purge the pending jobs.
`source`	One of: • `all` • `ondemand` • `rpc` • `device` • `fgt` • `fml` • `fct` • `fwb` • `sniffer` • `adapter` • `netshare` • `url` - URLs submitted through the On Demand page. • `urlrpc` - URLs submitted through JSON API. • `urldev` - URLs submitted from devices such as FortiMail. • `urlfgt` • `urlfml` • `urlfct` • `urlfwb` • `urladapter` • `urlsniffer` - URLs embedded in email body that are detected by sniffer.

Option	Description
`jobqueue`	One of: • `all` - All job queues. • `vm` - Sandobxing job queue. • `nonvm` - non-Sandboxing job queue. • `pre` - Files pending to enter job queue.
`filetype`	One of: • `all` • `exe` • `pdf` • `doc` • `flash` • `web` • `url` • `android` • `mac` • `user` • `other`

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, the user has to authorize it manually from the GUI.
`-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 FortiGate. or the user has to change it manually from the GUI.
`-f`	When a new FortiClient registers, FortiSandbox will authorize it automatically.
`-l`	Display the status of device and FortiClient authorization (default = manual).

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

Options

Either long or short options are allowed.

`--ipv4 -4`	Nothing (line is ignored by ip6tables-restore).

--ipv6 -6	Error (line is ignored by iptables-restore).
[!] --protocol -p proto	Protocol: by number or name, for example: tcp.
[!] --source -s address[/mask][...]	Source specification.
[!] --destination -d address[/mask][...]	Destination specification.
[!] --in-interface -i input name[+]	Network interface name ([+] for wildcard).
--jump -j target	Target for rule (may load target extension).
--goto -g chain	Jump to chain with no return.
--match -m match	Extended match (may load extension).
--numeric -n numeric	Output of addresses and ports.
[!] --out-interface -o output name[+]	Network interface name ([+] for wildcard).
--table -t table	Table to manipulate (default: `filter').
--verbose -v	Verbose mode.
--wait -w	Wait for the xtables lock.
--line-numbers	Print line numbers when listing.
--exact -x	Expand numbers (display exact values).
[!] --fragment -f	Match second or further fragments only.
--modprobe=<command>	Try to insert modules using this command.
--set-counters PKTS BYTES	Set the counter during insert/append.
[!] --version -V	Print package version.

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 a regular license.

hc-settings

Configure the unit as a HA-Cluster mode unit.

syntax

```
hc-settings <option> [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`	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.
`-se`	Enable traffic encryption between HA cluster members.
`-sd`	Disable traffic encryption between HA cluster members.

hc-slave

Configure the unit as a HA-Cluster slave unit.

syntax

```
hc-slave <option>
```

Option	Description
`-h`	Help information.
`-a`	Add the slave unit to the HA-Cluster.
`-r`	Remove the slave unit from the HA-Cluster.
`-u`	Update the slave unit information.
`-s`	The master unit IP address.
`-p`	The HA-Cluster authentication code.

hc-master

Configure the unit as a HA-Cluster master unit.

syntax

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

Option	Description
`-h`	Help information.
`-u`	Turn off file scan on master unit.
`-s<10-100>`	Turn on file scan on master unit with 10% to 100% processing capacity.
`-l`	Display the file scan status on master unit.
`-r<slave_sn>`	Remove the slave unit from the HA-Cluster by its serial number.

hc-status

Check HA-Cluster status.

syntax

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

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

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

vm-customized

Install a customized VM.

Syntax

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

Option		Description
`-h`		Help information.
`-c[n|l|f|d]`		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.
`-t<ftp|scp>`		The protocol type, FTP or SCP (default = scp).
`-s<server IP>`		Download the image file from this FTP or SCP server IP address.
`-u<user name>`		The user name for authentication.
`-f<full path of filename>`		The full path for the image file or meta file.
`-d<hardware/machine ID>`		The original hardware ID or machine ID.
`-k<MD5 checksum>`		The 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>`	The name of the VM.
`-r <VM name>`		Replace the VM if it already exists.

sandboxing-cache

Turn on or off the sandboxing result cache.

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.

Option	Description
`-l`	Reset local sandboxing result cache.
`-r`	Remove all existing cache results.

sandboxing-prefilter

Allow user to turn on or off FortiGuard prefiltering of 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. The user can turn on FortiGuard prefiltering of a file type so that files of that type will first be statically scanned 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]
```

Option	Description
`-h`	Help information.
`-e`	Enable sandboxing prefilter.
`-d`	Disable sandboxing prefilter.
`-l`	Display the status of sandboxing prefilter.
`-t`	Enable/disable sandboxing prefilter for specific file types: `archive`, `dll`, `pdf`, `swf`, `js`, `htm`, `url`, `office`, `trustvendor`, `trustdomain`. `archive` and `trustdomain` are enabled by default. Other prefilters are disabled by default. When `trustvendor` is selected, executable files from a small internal list of trusted vendors will skip the sandboxing scan step. When `trustdomain` is selected, files downloaded from a small internal list of trusted domains will skip the sandboxing scan step

sandboxing-embeddedurl

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

Syntax

```
sandboxing-embeddedurl <option>
```

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.

filesize-limit

Set file size limit of different input sources.

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, default = 200).
-u	Set the total uncompressed file size limitation for an archive file, in megabytes (0 - 2048, default = 500).

The upper bound for FSA_VM ondemand is 10240MB.

remote-auth-timeout

Set Radius or LDAP authentication timeout value.

Syntax

```
remote-auth-timeout <option>
```

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

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).

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.

Option	Description
-d<DNS server IP>	DNS server IP address.
-u	Unset VM internet configuration for port3.

raid-rebuild

Rebuild raid after a new HD replaces a bad one.

Syntax

```
raid-rebuild <options>
```

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

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.

set-maintainer

The maintainer account is used to reset users' passwords.

Syntax

```
set-maintainer <option>
```

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

set-tcp-timestamp-response

Enable or disable TCP timestamp response. Default is enable.

Syntax

```
set-tcp-timestamp-response <option>
```

Option	Description
`-h`	Help information.
`-l`	Show current TCP timestamp response setting.
`-e`	Enable TCP timestamp response.
`-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.

Option	Description
`-e`	Set the allowed TLS versions. `1` and `2` are for TLS 1.1 and 1.2 (default). Separate versions with `|`, for example `–e1|2` will enable TLS 1.1 and 1.2. TLSv1.0 is not supported.

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 <option>
```

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.

oftpd-con-mode

Enable/disable conserve mode of OFTPD.

Syntax

```
oftpd-con-mode <option>
```

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

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.

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: • `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
```

ai-mode

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

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

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

Syntax

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

Option	Description
`-h`	Help information.
`-l`	Display the current AI mode setting.
`-e`	Enable using AI logic to do job's behavior analysis.
`-d`	Disable using AI logic to do job's behavior analysis (default).

Utility Commands

The following utilities are available:

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

Diagnose Commands

The following diagnostic commands are available:

Command	Description
`hardware-info`	Display general hardware status information. Use this option to view CPU, memory, disk, and RAID information, as well as system time settings.
`diagnose-clilog`	Record all CLI input and output. See diagnose-clilog on page 27 for details.
`diagnose-krnlog`	Record the kernel ring buffer. See diagnose-krnlog on page 28 for details.
`diagnose-debug`	Display detailed debug logs of network share scan and communications with devices. See diagnose-debug on page 28 for details.
`diagnose-sys-top`	Display system top information. See diagnose-sys-top on page 29 for details.
`diagnose-sys-perf`	Display system performance information. Optionally, specify how many previous hours to show with `-m<hours>` (maximum = 40320, default = 1).
`disk-attributes`	Display system disk attributes. This option is only available on hardware models.
`disk-errors`	Display any system disk errors. This option is only available on hardware models.
`disk-health`	Display disk health information. This option is only available on hardware models.
`disk-info`	Display disk hardware status information. This option is only available on hardware models.
`raid-hwinfo`	Display RAID hardware status information. This option is only available on hardware models.
`test-network`	Test the network connection. The output can be used to detect network speed and connection to FDN servers and Microsoft servers.

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-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-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.

Option	Description
`adapter_icap`	Daemon for Internet Content Adaptation Protocol (ICAP).
`adapter_bcc`	Daemon for BCC.
`adapter_mta_relay`	Daemon for MTA Relay.
`adapter_mta_mail`	Daemon for MTA Mail.
`device_serial_number`	The device serial number.

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).
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

Change Log

Date	Change Description
2020-06-09	Initial release.