



FortiSandbox - CLI Reference Guide

Version 3.2.0

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 08, 2020

FortiSandbox 3.2.0 CLI Reference Guide

34-320-610768-20200608

TABLE OF CONTENTS

Introduction	5
What's New in FortiSandbox	6
Configuration Commands	7
System Commands	8
fw-upgrade	10
pending-jobs	11
device-authorization	12
iptables	13
usg-license	15
hc-settings	15
hc-slave	16
hc-master	16
hc-status	17
restore-sysconf	17
backup-sysconf	18
confirm-id	18
vm-customized	18
sandboxing-cache	19
sandboxing-prefilter	20
sandboxing-embeddedurl	21
filesize-limit	21
remote-auth-timeout	22
log-dropped	22
vm-internet	22
raid-rebuild	23
reset-sandbox-engine	23
set-maintainer	24
set-tlsver	24
fortimail-expired	24
oftpd-con-mode	25
device-lenc	25
upload-settings	26
ai-mode	26
set-cfg-backup-key	27
Utility Commands	28
Diagnose Commands	29
diagnose-clilog	29
diagnose-krnlog	30
diagnose-debug	30
diagnose-sys-top	31
test-network	31

Change Log33

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 commands and variables are new or have changed in version 3.2.0.

Command	Description
<code>set-cfg-backup-key [-h -s -r]</code>	Set your own passphrase that openSSL uses to encrypt or decrypt a configuration backup file.
<code>test-network [-h argument]</code>	Test the network connection. Use the output to detect network speed and connection to FDN servers and Microsoft servers. Testing FDN service and FSA community cloud service also show the IP address or server.
<code>raid-hwinfo</code>	This command now shows if auto RAID (AutoRebuild) is enabled or disabled.
<code>set-tlsver</code>	This version supports TLS 1.3.
<code>diagnose-debug</code>	This command has <code>adapter_mta_relay</code> and <code>adapter_mta_mail</code> options.

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

System Commands

Command	Description
reboot	Reboot the FortiSandbox. All sessions will be terminated. The unit goes offline and there is a delay while it restarts.
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.
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.
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	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 displays information to help troubleshoot the problem.
vm-reset	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.
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 10 .
reset-widgets	Reset the GUI widgets.
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.
log-purge	Delete all system logs.
pending-jobs	Show the status of or delete pending jobs. For details, see pending-jobs on page 11 .
device-authorization	Configure new client device authorization . For details, see device-authorization on page 12 .

Command	Description
<code>iptables</code>	Enable/disable IP tables. For details, see iptables on page 13 .
<code>usg-license</code>	Convert the unit to be USG licensed. For details, see usg-license on page 15 .
<code>hc-settings</code>	Configure the unit as a HA-Cluster mode unit. For details, see hc-settings on page 15 .
<code>hc-status</code>	List the status of HA-Cluster units.
<code>hc-slave</code>	Add/update/remove a slave unit to/from an HA-Cluster. This command can only be run on a slave unit.
<code>hc-master</code>	Enable/disable the malware detection features on master unit. 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.
<code>restore-sysconf</code>	Restore system configuration from remote server. For details, see restore-sysconf on page 17 .
<code>backup-sysconf</code>	Upload system configuration backup to remote server. For details, see backup-sysconf on page 18 .
<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>confirm-id</code>	Set confirm ID for Microsoft Windows or Office activation. For details, see confirm-id on page 18 .
<code>vm-customized</code>	Install customized VM. For details, see vm-customized on page 18 .
<code>sandboxing-cache</code>	Enable/disable sandboxing result check. For details, see sandboxing-cache on page 19 .
<code>reset-scan-profile</code>	Reset the clone number and file extension association back to firmware default values using the <code>-r</code> option.
<code>sandboxing-prefilter</code>	Enable/disable sandboxing prefilter for file types. For details, see sandboxing-prefilter on page 20 .
<code>sandboxing-embeddedurl</code>	Enable/disable feature for sandboxing embedded urls in PDF or OFFICE documents. For details, see sandboxing-embeddedurl on page 21 .
<code>filesize-limit</code>	Set file size limitation for scan input type, in megabytes (default = 200). For details, see filesize-limit on page 21 .
<code>remote-auth-timeout</code>	Set the timeout for remote authentication. For details, see remote-auth-timeout on page 22 .

Command	Description
log-dropped	Enable/disable the log file drop event. For details, see log-dropped on page 22 .
vm-internet	Allow Virtual Machines to access external network through outgoing port3 and set gateway for port3. For details, see vm-internet on page 22 .
cm-status	List the status of units joining the Global Threat Information Network.
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. This option is only available on hardware models. For details, see raid-rebuild on page 23 .
reset-sandbox-engine	Reset the tracer/rating engine back to firmware default. For details, see reset-sandbox-engine on page 23 .
set-maintainer	Enable/disable the maintainer account. For details, see set-maintainer on page 24 .
set-tlsver	Set the allowed TLS version for HTTPS service. For details, see set-tlsver on page 24 .
fortimail-expired	Enable/disable expired timeout option for FortiMail files. For details, see fortimail-expired on page 24 .
oftpd-con-mode	Enable/disable conserve mode of OFTPD. For details, see oftpd-con-mode on page 25 .
device-lenc	Enable/disable OFTPD supporting FortiGate-LENC devices. For details, see device-lenc on page 25 .
upload-settings	Configure data upload settings to community cloud. For details, see upload-settings on page 26 .
ai-mode	Enable/disable using AI logic to do job's behavior analysis. For details, see ai-mode on page 26 .
set-cfg-backup-key	Set your own passphrase that openssl uses to encrypt or decrypt a configuration backup file.

fw-upgrade

Upgrade or re-install the FortiSandbox firmware via SCP or FTP server. Before running this option, the firmware file should be downloaded to a server that supports file copy via FTP/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	<p>One of:</p> <ul style="list-style-type: none"> 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

Option	Description
	<ul style="list-style-type: none"> • 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

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.

Option	Description
-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.

<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.

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> [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.

Option	Description
<code>-i<interface></code>	Set interface used for cluster internal communication.
<code>-si</code>	Set the fail-over IPs for this cluster for master unit.
<code>-i<interface></code>	Specify the interface for external communication
<code>-a<IP/netmask></code>	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.
<code>-se</code>	Enable traffic encryption between HA cluster members.
<code>-sd</code>	Disable traffic encryption between HA cluster members.

hc-slave

Configure the unit as a HA-Cluster slave unit.

syntax

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

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

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.

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.

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.
-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	<p>Enable/disable sandboxing prefilter for specific file types: archive, dll, pdf, swf, js, htm, url, office, trustvendor, trustdomain.</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>

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.

Option	Description
-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.

raid-rebuild

Rebuild raid after a new HD replaces a bad one. This option is only available on hardware models.

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-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.

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: <ul style="list-style-type: none">• <code>uploadcloud</code>: Upload malicious and suspicious file information to Sandbox Community Cloud. Default is enabled.• <code>submiturl</code>: Submit suspicious URL to Fortinet WebFilter service. Default is disabled.• <code>uploadstats</code>: 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.

Option	Description
-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).

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 <option>
```

Option	Description
-h	Help information.
-s	Set configuration backup encryption key.
-r	Reset configuration backup encryption key to 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]
tracert	Examine the route taken to another network host: tracert <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 29 for details.
diagnose-krnlog	Record the kernel ring buffer. See diagnose-krnlog on page 30 for details.
diagnose-debug	Display detailed debug logs of network share scan and communications with devices. See diagnose-debug on page 30 for details.
diagnose-sys-top	Display system top information. See diagnose-sys-top on page 31 for details.
diagnose-sys-perf	Display system performance information. Optionally, specify how many previous hours to show with <code>-m<hours></code> (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, including if auto RAID (AutoRebuild) is enabled. This option is only available on hardware models.
test-network	Test the network connection. Use the output 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

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 <option>
```

Option	Description
-h	Help information.
local_resolve_speed	Test system DNS resolve
ping_speed	Test ping speed.
wget_speed	Test wget speed.
fdn	Test FDN service. The results show the IP address or server.
web_filter	Test Web Filtering service.
cloud	Test FSA community cloud service. The results show the IP address or server.
cloudvm	Test FSA Windows Cloud VM service.
vm_connect	Test VM Internet access via port3.
connect	Test system Internet connection.
resolve_speed	Test VM DNS resolve speed.

Change Log

Date	Change Description
2020-04-30	Initial release.
2020-06-08	Minor updates and corrections to multiple topics.



FORTINET®



Copyright© 2020 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.