FortiDeceptor - CLI Reference Guide

Version 1.1.0

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 COOKBOOK
https://cookbook.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: techdocs@fortinet.com

December 20, 2018
FortiDeceptor 1.1.0 CLI Reference Guide
50-110-530603-20181220

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-12-20	Initial release.

Introduction

The FortiDeceptor Command Line Interface (CLI) is accessed when connecting to the FortiDeceptor via console or using an SSH or TELNET client. These services must be enabled on the port1 interface.

The 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` to view a description of all of the available commands. Use `?` or `help` with a system command for information on how to use that command. Use `exit` to exit from the CLI.

An administrator's privilege to execute CLI commands is defined by their admin profile. The specific commands that are available to them are configured when creating or editing a profile.

The FortiDeceptor CLI is case-sensitive.

What's New in FortiDeceptor

The following table list the commands and variables that have changed in version 1.1.0.

Command	Change
`dmz-mode`	Command added

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.
set	Set configuration parameters. • `set portX-ip <ip/netmask>` - Set the portX IP address in IP/netmask format. • `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 default-gw	Unset the default gateway.

System Commands

The following system commands are available:

Command	Description
reboot	Reboot the FortiDeceptor. All sessions will be terminated. The unit will go offline and there will be a delay while it restarts.
shutdown	Shutdown the FortiDeceptor.
config-reset	Reset the configuration to factory defaults. Event and incident data are kept. Installed VM images are also kept.
factory-reset	Reset the FortiDeceptor configuration to factory default settings. All data are deleted. Installed VM images are kept.
status	Display the FortiDeceptor firmware version, serial number, system time, disk usage, image status, and RAID information.
fw-upgrade	Upgrade or re-install the FortiDeceptor firmware or deception VM image via Secure Copy (SCP) or File Transfer Protocol (FTP) server. See fw-upgrade on page 9 for details.
reset-widgets	Reset the GUI widgets.
iptables	Enable/disable IP tables. See iptables on page 9 for details.
dcvm-confirm-id	Set confirm ID for Windows deception VM activation. See dcvm-confirm-id on page 11 for details.
dcvm-license	List the license information for deception VMs using the `-l` option.
dcvm-status	Display the status for deception VMs.
dcvm-reset	Activate and initialize VM images 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.
dcimg-status	Display the status of deception images.
set-maintainer	Enable/disable the maintainer account. See set-maintainer on page 11 for details.
remote-auth-timeout	Set Radius or LDAP authentication timeout value. See remote-auth-timeout on page 12 for details.
log-purge	Delete all system logs.
vm-firmware-license	Download firmware license file from a server and install it. See vm-firmware-license on page 12 for details.

Command	Description
vm-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 VM models.
dmz-mode	Enable/disable the DMZ mode to deploy the unit into the DMZ environment.

fw-upgrade

Upgrade or re-install the FortiDeceptor firmware or deception VM image 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 | scp>	The protocol type, FTP or SCP (default =SCP).
-s<server IP address>	The IP address of the server that the image will be downloaded from.
-u<user name>	The user name for authentication.
-p<password>	The password for authentication.
-f<file path>	The full path for the image file.

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.

dcvm-confirm-id

Validate a Microsoft Windows key after contacting Microsoft customer support.

Syntax

```
dcvm-confirm-id <option> [options]
```

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

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.

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.
-l	Display the timeout value.

vm-firmware-license

Download firmware license file from a remote server and install it.

This command is only available for VM models.

Syntax

```
upload_license <options>
```

Option	Description
-s<server ip>	Download a license file from this server IP address.
-t<ftp | scp>	The protocol type, FTP or SCP (default =SCP).

Option	Description
-u<username>	The user name for server authentication.
-p<password>	The password for server authentication.
-f<license filename>	The full path for the license file.

Utility Commands

The following utilities are available:

Command	Description
ping	Test network connectivity to another network host: `ping <IP address>`
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.
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.