FortiDeceptor - CLI Reference Guide

Version 3.0.1

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

F:::RTINET®

TABLE OF CONTENTS

Introduction

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

Use CLI commands for initial device configuration and troubleshooting. CLI commands are case-sensitive. 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 the CLI.

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

Configuration Commands

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

Command	Description
reboot	Reboot the FortiDeceptor. All sessions are terminated, the unit goes offline, and there is a delay while it restarts.
shutdown	Shut down the FortiDeceptor.
config-reset	Reset the configuration to factory defaults. Event and incident data, and installed VM images are kept.
data-purge	Purge the detection results from the database, including deployment settings, events, incidents, and alerts.
factory-reset	Reset the FortiDeceptor configuration to factory default settings. All data is 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 7 for details.
reset-widgets	Reset the GUI widgets.
iptables	Enable/disable IP tables. See iptables on page 8 for details.
dcvm-confirm-id	Set confirm ID for Windows deception VM activation. See dcvm-confirm-id on page 10 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. This is useful when you need to rebuild a broken VM image. The default resets all VMs or you can specify a VM name with -n <VM name>.
dcimg-status	Display the status of deception images.
set-maintainer	Enable or disable the maintainer account. See set-maintainer on page 10 for details.
remote-auth-timeout	Set Radius or LDAP authentication timeout. See remote-auth-timeout on page 11 for details.
log-purge	Delete all system logs.
vm-firmware-license	Download and install the firmware license file from a server. See vm-firmware-license on page 11 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 or disable the DMZ mode to deploy the unit in a DMZ environment.
fdn-pkg	Display information about FortiGuard upgradeable engine packages.
test-network	Test the network connectivity of firmware.

data-purge

Syntax

```
data-purge <option>
```

Option	Description
-a	Purge all the data in the database including deployment settings, events, incidents, and alerts.
-d	Purge the detection results from database, including events, incidents, and alerts.

fw-upgrade

Upgrade or re-install the FortiDeceptor firmware or deception VM image via SCP or FTP server. Before running this option, download the firmware file onto 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
-b	Download an image file from this server and upgrade the firmware.
-v	Download and install a VM image file from this server.
-t<ftp | scp>	The protocol type, FTP or SCP (default).
-s<server IP address>	The IP address of the server to download the image.
-u<user name>	The user name for authentication.

Option	Description
`-p<password>`	The password for authentication.
`-f<file path>`	The full path of the image file.

iptables

Use this command to enable or disable IP tables. The settings are 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

You can use long or short commands.

`--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

You can use long or short commands.

`--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

Use the maintainer account to reset user passwords.

Syntax

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

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

vm-firmware-license

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

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).
-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

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

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.

Change Log

Date	Change Description
2020-02-14	Initial release.