CLI Reference Guide

FortiDeceptor 5.3.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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 LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

December 20, 2023
FortiDeceptor 5.3.0 CLI Reference Guide
50-530-978704-20231220

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-12-20	Initial release.

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. • `set tag ics` - Enable Mitre ICS tags.
`unset default-gw`	Unset the default gateway.
`unset tag`	Disable Mitre ICS tags.

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 9 for details.
`reset-widgets`	Reset the GUI widgets.
`dcvm-confirm-id`	Set confirm ID for Windows deception VM activation. See dcvm-confirm-id on page 9 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 10 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 10 for details.
`vm-resize-hd`	After changing the virtual hard disk size on the hypervisor, execute this command to make the change recognizable to the firmware.

Command	Description
	This command is only available for VM models.
`dmz-mode`	Enable or disable DMZ deployment mode.
`fdn-pkg`	Display information about FortiGuard upgradeable engine packages.
`storage-check`	Check storage disk with `fsck` command.
`storage-format`	Format storage disk.
`cm`	Central Manager configuration. See cm on page 11 for details.
`fabric-binding`	Set the Fabric traffic binding to port1. See fabric-binding on page 12 for details.

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.
`-t`	Purge campaigns that happened before a specific time (`MM/DD/YYYY-HH:MM:SS`). For example, to purge data by time use: `data-purge -d -t04/19/2021-12:15:35` You do not need to provide a timezone. FortiDeceptor will use the timezone configured on your device. If no timezone is set, FortiDeceptor will use UTC by default. For example, if the login user device is set to PDT timezone, running `data-purge -d -t04/19/2021-12:15:35` will purge the corresponding data before `04/19/2021-12:15:35` PDT. If the login user device is not set to a specific timezone, this command will purge corresponding data before `04/19/2021-19:15:35` UTC.
`-k<N>`	Automatically purges data older than the specified number of days where `N` represents `1-365` days. For example, to purge data older than 10 days : `data-purge -k10` This option cannot be used with other options.
`-s`	Show the configuration for automatic purge.

fw-upgrade

Upgrade or re-install the FortiDeceptor firmware or deception VM image via FTP, HTTPS, or SCP (default) server. Before running this command, download the firmware file onto a server that supports file copy via FTP, HTTPS, or SCP.

The system boots 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 | https | scp>`	The protocol type, FTP, HTTPS, or SCP (default).
`-s<ftp, https, or scp server IP address>`	The IP address of the server to download the image.
`-u<user name>`	The user name for authentication.
`-p<password>`	The password for authentication.
`-f<full file path>`	The full path of the image file.

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

```
vm-firmware-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.

cm

Central Manager configuration. This command is available for hardware and VM models.

The FortiDeceptor appliance can be configured in the following modes:

- Central Manager. Central Manager also has deception capability.
- Remote appliance (client).

Syntax

```
cm <options>
```

Option	Description
`-lc`	List the configuration of Central Manager mode unit.
`-ls`	List the status of Central Manager mode unit.
`-lj`	Optional. Output in JSON format.
`-sc -mC`	Set this unit to be a client mode (remote appliance).
`-sc -mM`	Set this unit to be a manager mode (Central Manager).
`-sc -n`	Set alias name for this unit (manager or client).
`-sc -a`	Set the authentication code for Central Manager communication.
`-sc -i`	Set the IP address of Central Manager server unit for client unit to connect.

Example

For example, in the following topology scenario:

- 1 Central Manager with IP address of 192.168.1.100
- 1 remote appliance (client) with IP address of IP:172.16.1.100

Use this configuration command on the manager side:

```
cm -sc -mM -nManager -a1234567890
```

Use this configuration command on the client side:

```
cm -sc -mC -nAppliance1 -a1234567890 -i192.168.1.100
```

fabric-binding

Set the Fabric traffic binding to port1. This command is available for hardware and VM models.

Syntax

```
  fabric-binding <options>
```

Option	Description
`-e`	Enable Fabric binding to port1.
`-d`	Disable Fabric binding to port1.
`-l`	Display the status of Fabric binding.

dcvm-license

Syntax

```
dcvm-license <option>
```

Option	Description
`-h`	Help information.
`-l`	List the deception VM license information.
`-lc`	List the deception contract information.
`-r[u|f]`	Remove the license/contract information manually. `-ru`: Remove the uploaded license information manually. `-rf`: Remove the FDN contract information manually.

passwd

Use this command to change the password of the current user. This CLI is for local users only, including read-only local users.

Syntax

```
passwd
```

Example:

```
> passwd
Old password: *************
New password: *************
Confirm password: *************
Successfully changed password, please re-login with the new password.
```

Diagnose commands

The following diagnostic commands are available:

- diagnose debug on page 14
- diagnose exec on page 14
- diagnose test on page 15

diagnose debug

Use this command to find out the root cause of system and network issues.

Syntax

```
diagnose debug <snmp | tidpassive | testnetwork | fabric>
```

Option	Description
`snmp`	Diagnose snmp agent issues.
`tidpassive`	Diagnose passive asset discovery.
`testnetwork`	Dagnose FDN connection issue
`fabric`	Diagnose fabric issues.

diagnose exec

Use this command to diagnose IP tables, network connectivity and network traffic.

Syntax

```
diagnose exec <iptables|ping|tcpdump>
```

Option	Description
`iptables <ARGS>`	Diagnose IP table issues.
`ping <HOST>`	Ping the IP addres.
`tcpdump <ARGS>`	Diagnose local network traffic.

Example:

```
diagnose exec ping 8.8.8.8

diagnose exec tcpdump -i port1 -c 10 host 192.168.0.123 and port 3128
diagnose exec tcpdump -h
```

diagnose test

Use this command to test the network and the deployment network.

Syntax

```
diagnose test <deployment-network | network>
```

Options	Description
`deployment-network <ARGS>`	Test the deployment network.
`network [-v|verbose]`	Test the network connectivity of firmware.

Example:

```
diagnose test deployment-network -iport2 -m11:22:33:44:55:66

diagnose test network verbose
```

Utility Commands

Command	Description
`traceroute`	Examine the route taken to another network host: `traceroute <host>`

Hardware commands

Command	Description
`hardware-info`	Display general hardware status information for all FortiDeceptor models. 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.

www.fortinet.com