



CIGENT Technology, Inc.

2211 Widman Way

Fort Myers, FL 33901

www.cigent.com

Cigent CLI User Guide

Document Reference Number: CLI-USR-GUIDE

Version: 1.0.9

Cigent CLI Utility

Overview

This utility is a standalone application designed to be used for configuring and interacting with Cigent solid state storage devices. The utility is available for Windows and Linux. The application interface is the same for both the Windows and the Linux versions. The utility must be run with administrative privileges due to the increased access rights required to interact with low level storage interfaces.

The following help message may be accessed at any time by running the application without any parameters.

```
c:\>CigentCLI
```

```
-----  
Drive Selection
```

```
-----  
Options -l and -d are mutually exclusive but one must be specified
```

```
-l # print a list of attached drives
```

```
-d <drive> # drive path or serial  
-----
```

```
PBA Support
```

```
-----  
For drives that are configured with Cigent PBA, the username  
must be specified
```

```
-user <username> # PBA username to use  
-----
```

```
Protection
```

```
-----  
-lock <password> <range> # lock specified range
```

```
-unlock <password> <range> # unlock specified range  
-----
```

```
Config
```

```
-----  
-init <password> # initialize drive for use (8-32 character password)
```

```
-add <password> <range> <size in GiB (0 for all available)> [-ntfs/-ext/-none] # add  
protected storage
```

```
Optional: -ntfs (format ntfs) / -ext (format ext) / -none (do not format)
```

```
If not specified, it will be formatted ext
```

```
-list <password> # list all configured ranges  
-----
```

```
Deconfig
```

```
-----  
-remove <password> <range> # remove protected storage !!DESTRUCTIVE TO RANGE!!
```

```
-deinit <password> # deinitialize drive using password !!DESTRUCTIVE TO ALL RANGES!!
```

```
-psid_revert <psid> # fully erase drive using PSID !!DESTRUCTIVE TO ENTIRE DRIVE!!
```

```
-erase <password> # fully erase drive using password !!DESTRUCTIVE TO ENTIRE DRIVE!!  
-----
```

```
Example Usage  
-----
```

Initialize drive, add a 20GB ntfs formatted range, and unlock it:
CigentCLI -d \\.\PHYSICALDRIVE1 -init mypassword
CigentCLI -d \\.\PHYSICALDRIVE1 -add mypassword 1 20 -ntfs
CigentCLI -d \\.\PHYSICALDRIVE1 -unlock mypassword 1
Unlock a range on a Cigent PBA drive:
CigentCLI -d \\.\PHYSICALDRIVE1 -user myuser -unlock mypassword 1

Linux Configuration

If a SATA Cigent drive is to be used with a Linux operating system, the following parameter must be passed to the grub command line:

```
libata.allow_tpm=1
```

If desired, modify /etc/default/grub and add it to GRUB_CMDLINE_LINUX_DEFAULT

Example:

Change: GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
To: GRUB_CMDLINE_LINUX_DEFAULT="quiet splash libata.allow_tpm=1"

Run update-grub and reboot after making the change. Some systems may require a full power cycle for the change to take effect.

Scanning for Drives

The first step before interacting with a Cigent drive is to scan for them on the system. The device scan will only search for and list Cigent storage devices.

```
c:\>CigentCLI -l
```

```
1) Model: [PCIe SSD] S/N: [R6E10872090F00000012] FW: [SCFL13.1] Path:  
[\\.\PHYSICALDRIVE1]
```

Once the desired device is located, it can be specified on the command line using the *-d* switch. The drive may be specified by its path or by its serial number. Every command, with the exception of the *-l* command, requires that a drive be specified.

```
-d \\.\PHYSICALDRIVE1
```

```
-d R6E10872090F00000012
```

Cigent Pre-Boot Authentication Support

The Cigent CLI utility has support for drives configured with a Cigent PBA. In order to work with a PBA drive, the username must be specified. To specify a PBA username, the *-user* option may be used. The example below shows how to unlock range 1 on a PBA configured drive.

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -user myuser -unlock mypassword 1
```

Protection Functions

Locking and Unlocking Protected Storage

Read/write access to each range may be configured using the *-lock* and *-unlock* commands.

Lock

Locking a range will unmount the volume associated with it (if applicable) and will lock the range at the drive level to prevent read/write access.

Parameters: -lock <password> <range number>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -lock mypassword 1
```

Unlock

Unlocking a range will unlock the range at the drive level to allow read/write access and mount the volume associated with it (if applicable).

Parameters: -unlock <password> <range number>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -unlock mypassword 1
```

Configuration Functions

Initialization

The security subsystem must be initialized first. The provided password must be between 8 and 32 characters.

Parameters: -init <password>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -init mypassword
```



If your drive is already configured with Cigent PBA the -init function is not used

Adding Protected Storage

The drive supports 8 ranges that may be configured across the full span of the drive. Protected storage volumes may be set up using these locking ranges. Protected storage volumes function just like any other formatted storage volume with the added benefit that they may be locked and unlocked at the device level. They may also be quickly erased/removed. Protected Storage volumes are created by aligning a protected storage range on the same range occupied by a data partition. This allows the content of the partition to be protected using the various range protection options.

Parameters: -add <password> <range number> <size in GiB: 0 for all available> [-ntfs/-ext/-none]

File system options:

- -ntfs: format the drive using an NTFS file system
- -ext: format the drive using an EXT file system
- -none: do not format the drive (this will create an empty partition with no file system)

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -add mypassword 1 20 -ntfs
```



If you do not pick from one of the available file system options (-ntfs/-ext/-none) the storage will be formatted using a operating system dependent default (NTFS for Windows, EXT for Linux)



The -ext option is only available on Linux.
The -ntfs option is available on Windows as well as Linux systems that support NTFS.

Displaying Range Configuration

The current range configuration may be displayed using the -list command. The *Range* number is the identifier that is used to specify the range to interact with. The command will also display if the range is locked or unlocked. Lastly, a count of the number of ranges currently in use and the total available will be displayed.

Parameters: -list <password>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -list mypassword
```

Configured Ranges

Range 1: Locked

Range 2: Unlocked

2 of 8 ranges used

Deconfiguration Functions

Various data and configuration removal methods are available from full drive deinitialization to targeted range erasures and removals. A PSID revert method has also been provided that will allow the data to be erased in the event the drive password is forgotten.

Removing Protected Storage



This function will destroy all data on the specified range.

Protected Storage volumes are created by aligning a protected storage range on the same range occupied by a data partition. This function removes the partition as well as the protected storage range that is aligned with it.

Parameters: -remove <password> <range number>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -remove mypassword 1
```

De-Initializing Security Subsystem



This function will destroy all data on all configured ranges

Protected Storage volumes are created by aligning a protected storage range on the same range occupied by a data partition. This function removes ALL range aligned partitions as well as the protected storage range that is aligned with them. Data that is not in a secure range will NOT be removed.

Parameters: -deinit <password>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -deinit mypassword
```

PSID Revert



This function will destroy all data on the drive.

The *PSID Revert* function erases and removes all ranges, ALL data on the drive, and deinitializes the security subsystem. The PSID is a value printed on the drive and can be used to erase the data in the event the drive password has been forgotten.

Parameters: -psid_revert <psid>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -psid_revert 8484832FJDFASVNVJ3834R94R4TVJNF2
```

Erase



This function will destroy all data on the drive.

The *Erase* function erases and removes all ranges, ALL data on the drive, and deinitializes the security subsystem. This function begins by performing a cryptographic erase. On supported drives/systems, the cryptographic erase will be followed by a full block level erase and an erasure verification will be performed. The utility will also output the status of the blocks for drives that support erasure verification. Please note that on setups that do not support full block level erasures, the erasure verification will fail (however the result of the cryptographic erasure will be reported). Full block erasures are supported with the following setups:

- Any Cigent drive that is mounted internally in a Linux based system

- Version 2 of any Cigent drive that is mounted internally or in a USB enclosure on a Windows or Linux based system

Parameters: -erase <password>

```
c:\>CigentCLI -d \\.\PHYSICALDRIVE1 -erase mypassword
```