Setting up an M.2 module for Opal Compliance
by using the SEDutil self-encrypting drive utility

Contents

1. Overview

This Application Note describes the setup of an M.2 module for Opal Compliance, by using the SEDutil self-encrypting drive utility.

A CD containing the software utilities used in this application note is available from Concurrent Technologies, order code SW UTL/006-05.

2. Initial Requirements

List of equipment required:

- Concurrent Technologies AD150/001 M.2 module with Opal support
- Concurrent Technologies board with M.2 socket, chassis, and power supply
- Monitor with suitable power cable and display cable
- USB Hub
- USB keyboard
- USB Flash drive

3. Download SEDutil Rescue Image

To begin the setup process, a rescue image is required. The supporting software CD includes example rescue images configured for different console devices (video, COM1, COM2…), the name of each image reflects the console for which they have been pre-configured.

Alternatively, an image can be retrieved from the SEDutil website:

http://github.com/ChubbyAnt/sedutil/releases

The image name used for this demonstration is:

RESCUE64-1.15.1-44-ge29fbb1.img

4. Create Bootable USB Drive

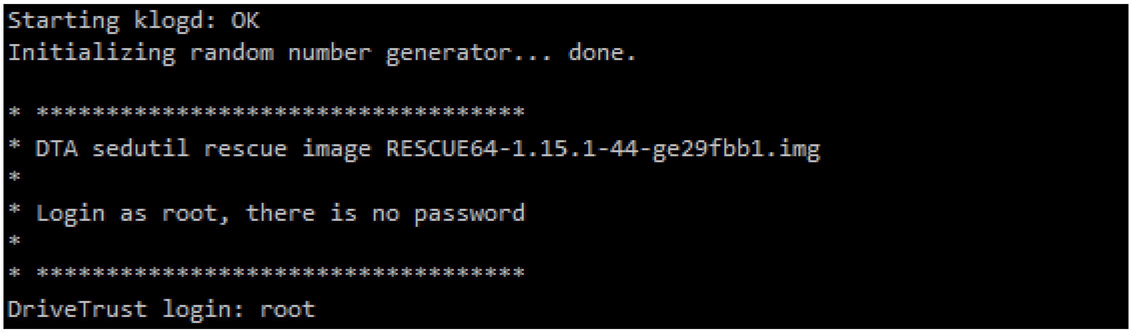
Using the image chosen in Section 3, a bootable USB drive can be created. This demonstration utilizes a software program called ‘Balena Etcher’ to prepare the USB drive. This program can be accessed and downloaded at the following address:

http://www.balena.io/etcher

Open ‘Balena Etcher’ and select the SEDutil image file chosen in Section 3. Select your blank USB, as the destination, and click on ‘flash’ to create the bootable USB.

5. Boot SEDutil Image

Plug the USB into the board with the OPAL M.2 and boot to the USB with the rescue image.



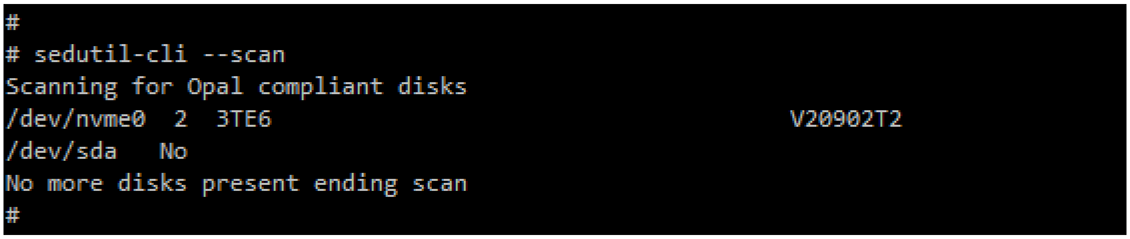
```
Starting klogd: OK
Initializing random number generator... done.

* ************************************
* DTA sedutil rescue image RESCUE64-1.15.1-44-ge29fbb1.img
*
* Login as root, there is no password
*
* ************************************
DriveTrust login: root
```

Type “root” and press enter to login. At this stage of the setup process, there is no password.

6. Scan the Drives

Type the following command: **`sedutil-cli --scan`**

Expected Output:



```
#
# sedutil-cli --scan
Scanning for Opal compliant disks
/dev/nvme0  2  3TE6                                     V20902T2
/dev/sda   No
No more disks present ending scan
#
```

WARNING

To verify that the drive is Opal 2.0 supported, ensure that the drive has a 2 in the second column. If it doesn't, **do not proceed**. There is something that is preventing SEDutil from supporting your drive. If you continue you may **erase all of your data.**

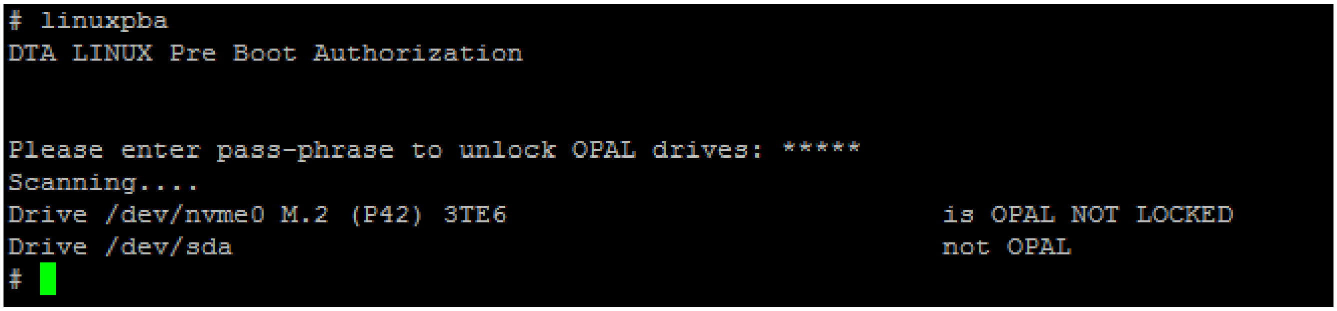
7. Test the Pre-boot Authentication (PBA)

Enter the command: **`linuxpba`**

Use the pass-phrase: **`debug`**

NOTE If you don't use **`debug`** as the pass-phrase your system will reboot.

Expected Output:

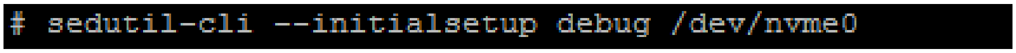


```
# linuxpba
DTA LINUX Pre Boot Authorization


Please enter pass-phrase to unlock OPAL drives: *****
Scanning....
Drive /dev/nvme0 M.2 (P42) 3TE6                           is OPAL NOT LOCKED
Drive /dev/sda                                            not OPAL
#
```

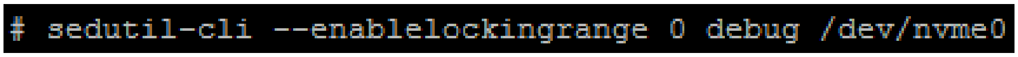
8. Enable Locking and the PBA

NOTE The following steps use **`/dev/nvme0`** as the drive and **`CCT_UEFI64_ttyS1.img.gz`** for the PBA image. You can substitute the appropriate **`drive`** and the PBA image for your system. The PBA image is on the USB flash drive that was created in Section 4. The file name of the PBA image will be dependent on the file you chose to create the USB with in Section 4.

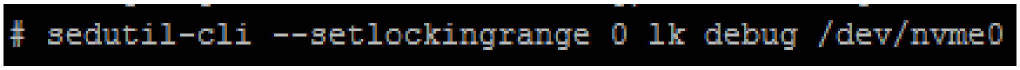
Enter the commands below: (Use the password debug for this test, it will be changed later)



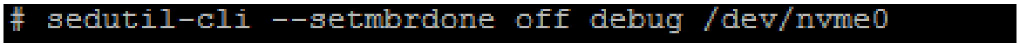
```
# sedutil-cli --initialsetup debug /dev/nvme0
```



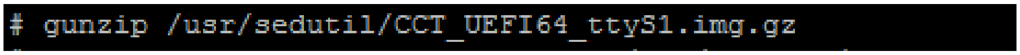
```
# sedutil-cli --enablelockingrange 0 debug /dev/nvme0
```



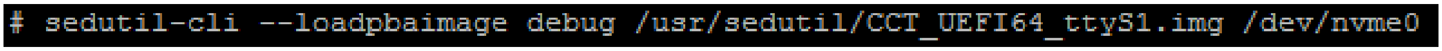
```
# sedutil-cli --setlockingrange 0 lk debug /dev/nvme0
```



```
# sedutil-cli --setmbrdone off debug /dev/nvme0
```

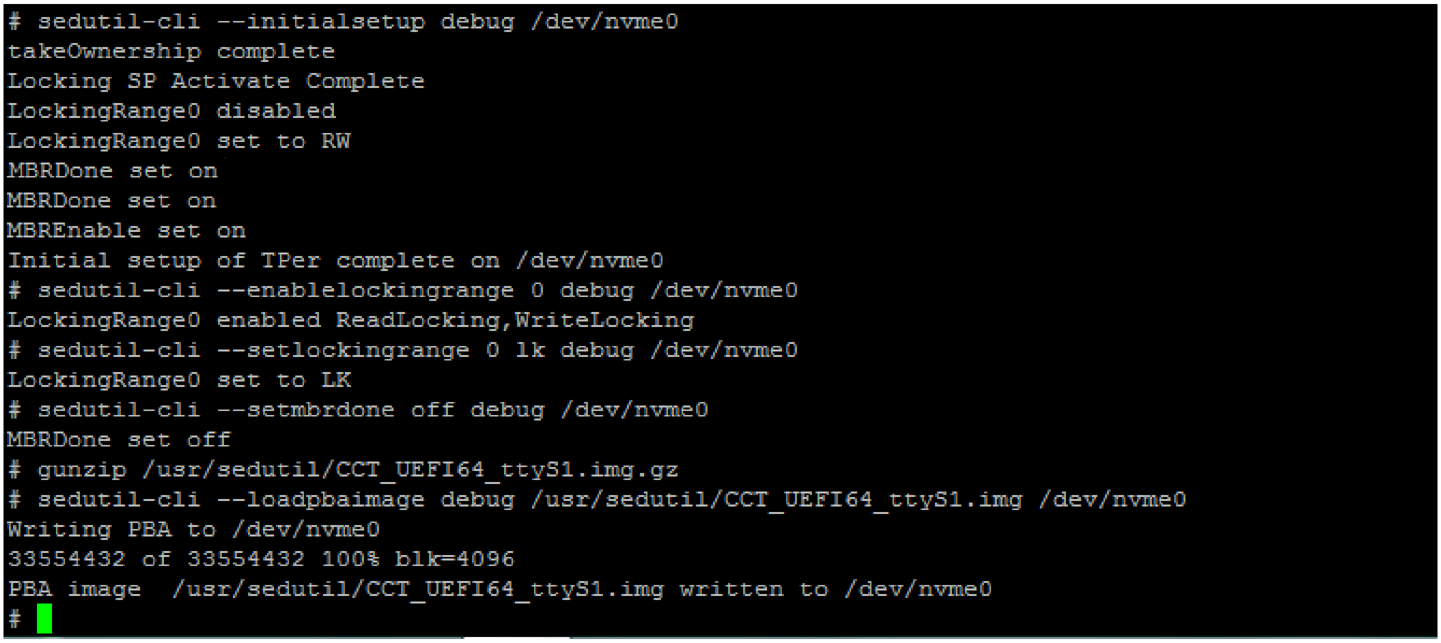


```
# gunzip /usr/sedutil/CCT_UEFI64_ttyS1.img.gz
```



```
# sedutil-cli --loadpbaimage debug /usr/sedutil/CCT_UEFI64_ttyS1.img /dev/nvme0
```

NOTE Please note the character used to enable locking range is the number ‘0’, not to be confused with letter ‘O’. When setting the locking range use the number ‘0’ and the letters ‘lk’.

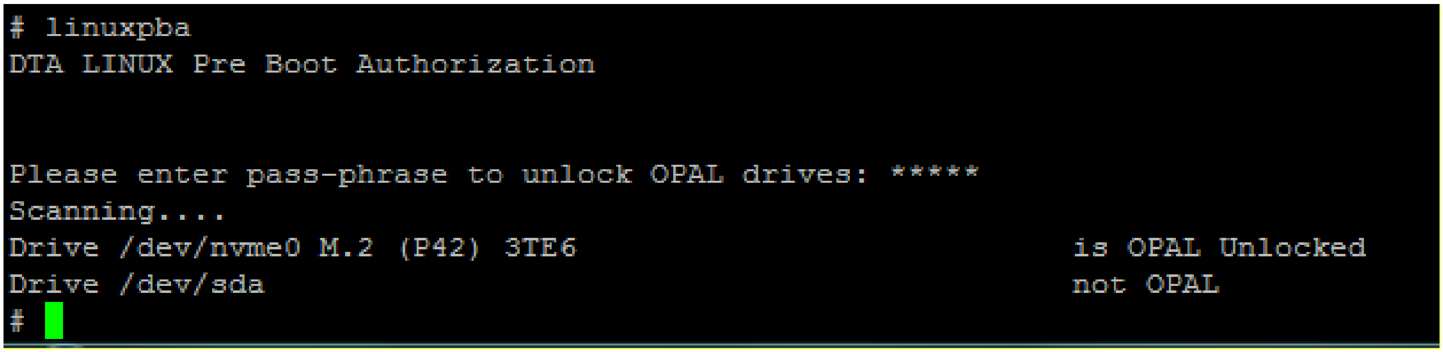


```
# sedutil-cli --initialsetup debug /dev/nvme0
takeOwnership complete
Locking SP Activate Complete
LockingRange0 disabled
LockingRange0 set to RW
MBRDone set on
MBRDone set on
MBREnable set on
Initial setup of TPer complete on /dev/nvme0
# sedutil-cli --enablelockingrange 0 debug /dev/nvme0
LockingRange0 enabled ReadLocking,WriteLocking
# sedutil-cli --setlockingrange 0 lk debug /dev/nvme0
LockingRange0 set to LK
# sedutil-cli --setmbrdone off debug /dev/nvme0
MBRDone set off
# gunzip /usr/sedutil/CCT_UEFI64_ttyS1.img.gz
# sedutil-cli --loadpbaimage debug /usr/sedutil/CCT_UEFI64_ttyS1.img /dev/nvme0
Writing PBA to /dev/nvme0
33554432 of 33554432 100% blk=4096
PBA image  /usr/sedutil/CCT_UEFI64_ttyS1.img written to /dev/nvme0
#
```

9. Test the PBA Again

To verify that the device does get unblocked, enter the command **`'linuxpba'`** and use a pass-phrase of **`'debug'.`**

Expected Output:



```
# linuxpba
DTA LINUX Pre Boot Authorization


Please enter pass-phrase to unlock OPAL drives: *****
Scanning....
Drive /dev/nvme0 M.2 (P42) 3TE6                          is OPAL Unlocked
Drive /dev/sda                                           not OPAL
#
```

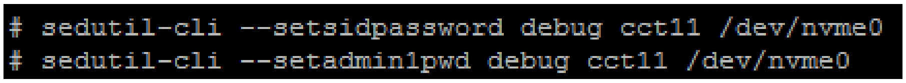
NOTE To verify that the PBA unlocks your drive, check that it says "is OPAL Unlocked". If this doesn't occur, follow the steps at the end of this Application Note to either remove OPAL or disable locking.

10. Set a Real Password

For ease of access, we recommend making the SID and Admin1 passwords match. However, this step is not essential.

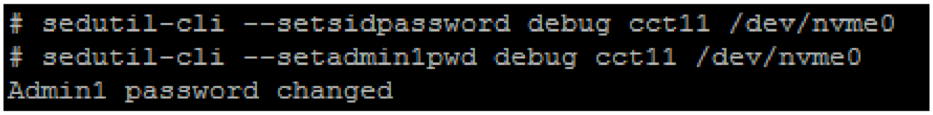
This example uses the password: **`cct11`**

Input:



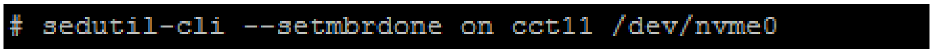
```
# sedutil-cli --setsidpassword debug cct11 /dev/nvme0
# sedutil-cli --setadmin1pwd debug cct11 /dev/nvme0
```

Expected Output:



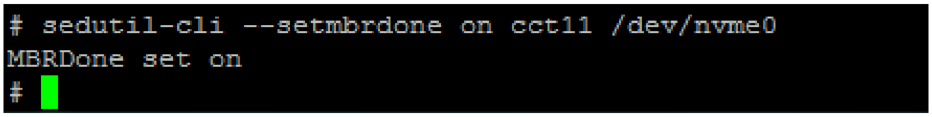
```
# sedutil-cli --setsidpassword debug cct11 /dev/nvme0
# sedutil-cli --setadmin1pwd debug cct11 /dev/nvme0
Admin1 password changed
```

To ensure that you have entered the correct password, you can perform a test by inputting the following:



```
# sedutil-cli --setmbrdone on cct11 /dev/nvme0
```

Expected Output:



```
# sedutil-cli --setmbrdone on cct11 /dev/nvme0
MBRDone set on
#
```

11. Complete the Process

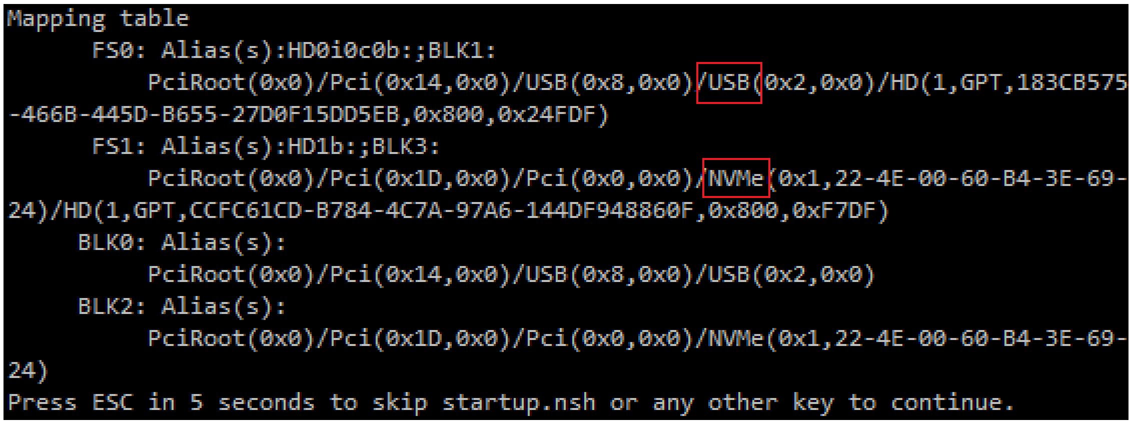
Because the installation of the PBA creates a new boot device, this will not have a UEFI boot entry and it will be necessary to create the UEFI boot entry. The utility CD includes an EFI application, shell.efi, that can be used to create a boot entry.

Copy shell.efi to a FAT32 formatted USB disk and insert the USB disk into one of the board's USB connectors.

Completely Power Down your system and power up again. This will lock the NVMe drive and ensure that the PBA device will be the active boot device. When the board comes back up, press <F12> and select the option to boot the "`Internal EFI Shell`".

Once the shell has started, look through the list of mapped drives and locate the USB and NVMe drive names.

Example drive mapping



```
Mapping table
      FS0: Alias(s):HD0i0c0b:;BLK1:
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0x8,0x0)/USB(0x2,0x0)/HD(1,GPT,183CB575
-466B-445D-B655-27D0F15DD5EB,0x800,0x24FDF)
      FS1: Alias(s):HD1b:;BLK3:
          PciRoot(0x0)/Pci(0x1D,0x0)/Pci(0x0,0x0)/NVMe(0x1,22-4E-00-60-B4-3E-69-
24)/HD(1,GPT,CCFC61CD-B784-4C7A-97A6-144DF948860F,0x800,0xF7DF)
     BLK0: Alias(s):
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0x8,0x0)/USB(0x2,0x0)
     BLK2: Alias(s):
          PciRoot(0x0)/Pci(0x1D,0x0)/Pci(0x0,0x0)/NVMe(0x1,22-4E-00-60-B4-3E-69-
24)
Press ESC in 5 seconds to skip startup.nsh or any other key to continue.
```

The example shows the USB drive name as `fs0` and the NVMe device name as `fs1`. These are outlined in red on the image on the previous page.

Change to the USB drive by typing the USB drive name followed by a colon (:)

```
    fs0:
```

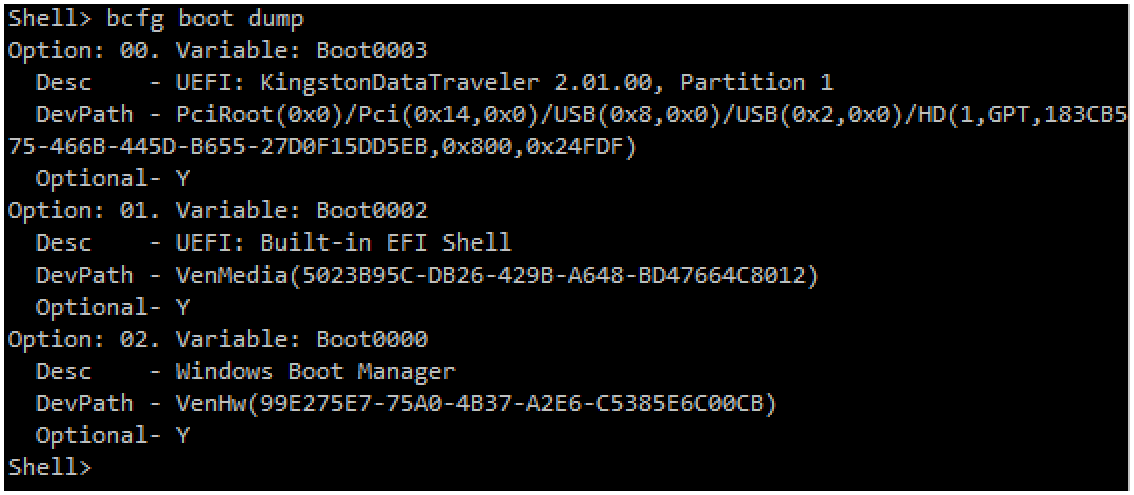
Start the new shell utility:

```
    shell.efi
```

Type the following command to display the current EFI boot entries:

```
    bcfg boot dump
```

Example output



```
Shell> bcfg boot dump
Option: 00. Variable: Boot0003
  Desc    - UEFI: KingstonDataTraveler 2.01.00, Partition 1
  DevPath - PciRoot(0x0)/Pci(0x14,0x0)/USB(0x8,0x0)/USB(0x2,0x0)/HD(1,GPT,183CB5
75-466B-445D-B655-27D0F15DD5EB,0x800,0x24FDF)
  Optional- Y
Option: 01. Variable: Boot0002
  Desc    - UEFI: Built-in EFI Shell
  DevPath - VenMedia(5023B95C-DB26-429B-A648-BD47664C8012)
  Optional- Y
Option: 02. Variable: Boot0000
  Desc    - Windows Boot Manager
  DevPath - VenHw(99E275E7-75A0-4B37-A2E6-C5385E6C00CB)
  Optional- Y
Shell>
```

Examine the output and find the highest Option number, we will use a value one higher than this to create a new UEFI boot entry in the next step. The general form of the command is as follows:

```
    bcfg boot add <highest ID plus 1> <NVMe drive name>:\EFI\boot\bootx64.efi "Opal PBA"
```

Using the NVMe drive name and Option number from the examples above, the command to create the new UEFI boot option would be:

```
    bcfg boot add 3 fs1:\EFI\boot\bootx64.efi "Opal PBA"
```

This creates a new EFI boot entry for the PBA boot device with the name `Opal PBA`.

Power Down your system and remove the USB drive. Power up again and when the board starts press <F2> to enter the BIOS Setup menus. Adjust the boot order so that `Opal PBA` is the first boot option. Save the changes and exit Setup.

Your board will boot the PBA image upon restart.

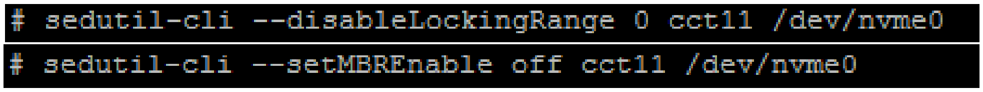
Once the PBA launches, type in the OPAL password that you created, in Section 9, the drive will unlock and the board will reboot. When the board reboots it is advisable to re-enter the BIOS setup and confirm that the OS image is the first boot device.

NOTE If board boots to the shell on the next power cycle you can disable the `Internal Shell` boot menu entry from the BIOS Setup `Boot` menu.

12. Recovery Information

If there is an issue after enabling locking, you can either disable locking or remove OPAL to continue using your drive without locking.

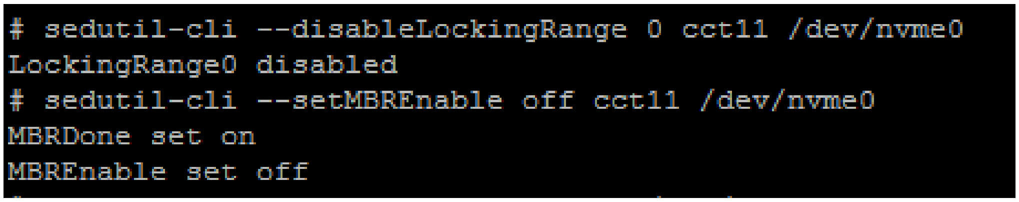
Disable Locking and the PBA:



```
# sedutil-cli --disableLockingRange 0 cct11 /dev/nvme0
# sedutil-cli --setMBREnable off cct11 /dev/nvme0
```

NOTE The drive must be unlocked before using these commands.

Expected Output:



```
# sedutil-cli --disableLockingRange 0 cct11 /dev/nvme0
LockingRange0 disabled
# sedutil-cli --setMBREnable off cct11 /dev/nvme0
MBRDone set on
MBREnable set off
```

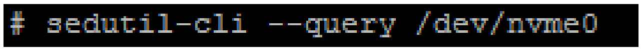
To remove Opal locking

To remove Opal locking you can perform a PSID revert.

WARNING Performing a PSID revert will render all data unrecoverable, so ensure all data is backed up before performing this step.

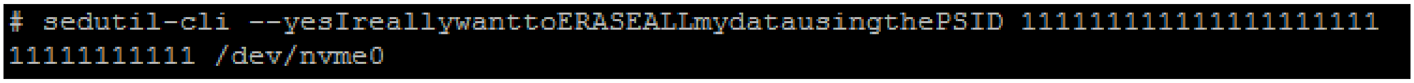
To perform a PSID revert follow the steps below:

1. Back up any user data to an alternate media source.
2. Query the security state of the drive by entering the following command:



```
# sedutil-cli --query /dev/nvme0
```

3. Note the **"Locking"** and **"Locking Enabled"** state of the drive. If the drive is locked the PSID revert should clear it.
4. Perform a PSID revert by entering the following command, using the PSID number on your label of your M.2 (in this example the PSID number is all 1s):



```
# sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID 11111111111111111111
11111111111 /dev/nvme0
```

5. Verify the command completed successfully.

13. If You Encounter Problems

If you encounter any problems while following the steps in this Application Note, you could attempt a PSID revert to reset the device. When this is finished your drive will now be in a non-opal-managed state.

Further information can also be found on the SEDutil WIKI page at:

https://github.com/Drive-Trust-Alliance/sedutil/wiki

NOTE: Information furnished by Concurrent Technologies is believed to be accurate and reliable. However, Concurrent Technologies assumes no responsibility for any errors contained in this document and makes no commitment to update or to keep current the information contained in this document. Concurrent Technologies reserves the right to change specifications at any time without notice. Concurrent Technologies assumes no responsibility either for the use of this document or for any infringements of the patent or other rights of third parties which may result from its use. In particular, no license is either granted or implied under any patent or patent rights belonging to Concurrent Technologies. All companies and product names are trademarks of their respective companies.

For additional information, please visit http://www.gocct.com

CONCURRENT
TECHNOLOGIES