

swissbit®

Application Note

AN4102en

**Set Up Opal Drives with
SEDutil**

© Swissbit AG 2025

 Creative Commons License¹

¹ This work is licensed under the Creative Commons License "Attribution 4.0 International". To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>

Contents

- 1 Abstract** **2**
- 2 TCG Opal** **2**
 - 2.1 TCG Opal introduction **2**
 - 2.2 TCG Opal Key Features **2**
- 3 SEDutil Tool** **3**
 - 3.1 Drive preparation **3**
 - 3.2 Check OPAL Support **3**
 - 3.3 Take Ownership to the drive **4**
 - 3.4 Enable the locking range **4**
 - 3.5 Set up the locking range **5**
 - 3.6 Test the locking range **6**
 - 3.7 Reset the drive to Default **6**
- 4 Summary** **6**

set of security specifications used for applying hardware-based encryption for storage devices.

2.2 TCG Opal Key Features

Hardware-based Encryption

Usually referred to as self-encrypting drive (SED). Self-encrypting drives adhering to the TCG OPAL 2.0 standard specification implement key management via an authentication key, and a 2nd-level data encryption key. The data encryption key is the key against which data on the drive is encrypted. The authentication key is the user-facing 1st-level passphrase which decrypts the data encryption key (which in turn decrypts the data). On this basis, SED has the following advantages:

1. Ease of deployment compared to software-based encryption
2. Simple key management
3. Optimized performance (No CPU utilization for encryption operations)
4. Data at rest protection
5. Instant secure erases (deleting encryption keys instead of time-consuming overwrites)

1 Abstract

TCG Opal is a security standard specification developed by the Trusted Computing Group (TCG), which defines security policies for data at rest protection, including Self-Encrypting drives (SEDs), user rights management and pre-boot authentication etc.

SEDutil (Self-Encrypting Drive Utility) is an open-source software tool designed for managing self-encrypting drives (SEDs). It provides functionality for working with storage devices that support the TCG Opal specification.

This document describes setting up a Swissbit TCG Opal drives with a tool called SEDutil. It covers the basics of the TCG Opal specification, the "sedutil" tool and introduces the specific use of SEDutil to identify Opal drives, set passwords, set ranges, and lock and unlock drives.

Shadow Master Boot Record (MBR)

The Shadow Master Boot Record (Shadow MBR) is a designated, small area (usually around 128 MB) on a TCG Opal-compliant encrypted drive. Its main function is to host the Pre-Boot Authentication (PBA) software that enables secure user authentication before the main contents of the drive are unlocked. Despite its name, the shadow MBR is not simply a boot record. Rather, it is a separate, isolated area that the host system can access before unlocking the encrypted parts of the drive.

Before authenticating, the Shadow MBR is write-protected, ensuring that only the PBA software is executed without any possibility of modification.

2 TCG Opal

2.1 TCG Opal introduction

Developed by the Trusted Computing Group (TCG), a not-for-profit international standards organization. The TCG Opal specification is a

Once the drive is unlocked, the shadow MBR, as the name implies, is usually hidden, meaning that a virus or the operating system itself would not be able to read or make changes to it. Since the shadow MBR is not visible on the drive, it is not accessible for standard operations, but it can be read or written to via special Opal ATA commands.

Once the drive loses power, the Shadow MBR will revert to its initial, pre-authentication state, and replace the normal MBR when read requests are made and any write requests will simply fail.

Locking Range Setting

An LBA Range is defined as a contiguous set of Logical Block Addresses (LBAs) that can be referenced as a single unit for operations such TRIM (Data set management), SANITIZE operations.

The locking LBA range is defined as a contiguous logical block range to store encrypted user data based on the rules:

1. Ranges don't overlap.
2. The first range (or range 0) is the global range that encompasses all LBAs which are not in the Shadow MBR.
3. When a range is created, a new encryption key is linked to this range, and all data that enters the range is encrypted or decrypted with this key.
4. A range can be crypto erased by re-encrypting it, which will change the encryption key for that range.
5. Each range can be set to be Read or Write Protect Enabled.

3 SEDutil Tool

SEDutil is an open source set of tools that provides locking and unlocking of TCG OPAL boot and non-boot drives in Windows and Linux. As below are the instructions about how to use SEDutil for setting up TCG Opal

drives. For a detailed explanation of specific commands of the tool please refer to the link: <https://manpages.debian.org/testing/sedutil/sedutil-cli.8.en.html>

Warning: Back up your entire drive before performing any operation. If you follow these instructions, you may lose all your data.

3.1 Drive preparation

A Swissbit PCIe NVMe SSD series like N2000 m.2 drive with the Opal compliant is used for the demo test (see below). The test system is PRIME Z390-A + Debian GNU/Linux 10. In this demo test, the N2000 drive is connected to the host system via an m.2 PCIe SSD Adapter.

NOTE: Compared to the NVMe drive, there is a slight difference when using the tool to set up the SATA drive with the Opal compliant, which is, libata.allow_tpm must be set to 1 (true) to use SEDutil. Either add libata.allow_tpm=1 to the kernel parameters, or by setting /sys/module/libata/parameters/allow_tpm to 1.

3.2 Check OPAL Support

Use the command below to scan the drive in the host system and check for OPAL compliant drives. Verify that there is a 2 in the second column indicating OPAL 2 supported.

```
$ sudo ./sedutil-cli --scan
Scanning for Opal compliant disks
/dev/nvme0 2 SN2000MD480GI-1TB8-1DB-STD 2
└─ ECR50001
```

The drive can be queried for its supported features, see command below. Note that the encryption is currently not enabled (LockingEnabled = N) but supported (LockingSupported = Y) and the MBR (Master Boot Record) shadowing is not enabled. The logical block size of the drive is 512bytes. It can support 4 admin accounts and 9 user accounts.

```
$ sudo ./sedutil-cli --query /dev/nvme0:
```

```

/dev/nvme0 NVMe ↵
└─ SN2000MD480G1-1TB8-1DB-STD ECR50001 ↵
└─ 000099005519EF00001
TPer function (0x0001)
  ACKNAK = N, ASYNC = N. BufferManagement ↵
└─ = N, comIDManagement = N, Streaming ↵
└─ = Y, SYNC = Y
Locking function (0x0002)
  Locked = N, LockingEnabled = N, ↵
└─ LockingSupported = Y, MBRDone = N, ↵
└─ MBREnabled = N, MediaEncrypt = Y
Geometry function (0x0003)
  Align = Y, Alignment Granularity = 1 (512), ↵
└─ Logical Block size = 512, Lowest Aligned ↵
└─ LBA = 0
SingleUser function (0x0201)
  ALL = N, ANY = N, Policy = Y, Locking Objects ↵
└─ = 9
DataStore function (0x0202)
  Max Tables = 10, Max Size Tables = ↵
└─ 10485760, Table size alignment = 1
OPAL 2.0 function (0x0203)
  Base comID = 0x0888, Initial PIN = 0x00, ↵
└─ Reverted PIN = 0x00, comIDs = 1
  Locking Admins = 4, Locking Users = 9, ↵
└─ Range Crossing = N
**** 1 **** Unknown function codes IGNORED
TPer Properties:
  MaxComPacketSize = 32256 ↵
└─ MaxResponseComPacketSize = 32256
  MaxPacketSize = 32236 MaxIndTokenSize = ↵
└─ 32200 MaxPackets = 1
  MaxSubpackets = 1 MaxMethods = 1 ↵
└─ MaxSessions = 1
  MaxAuthentications = 14 MaxTransactionLimit ↵
└─ = 1 DefSessionTimeout = 500000
  MaxSessionTimeout = 0 MinSessionTimeout = ↵
└─ 5000
Host Properties:

MaxComPacketSize = 2048 MaxPacketSize = ↵
└─ 2028 MaxIndTokenSize = 1992
  MaxPackets = 1 MaxSubpackets = 1 ↵
└─ MaxMethods = 1

```

3.3 Take Ownership to the drive

Taking control of the drive is completed by the process of “take Ownership”. Using the command below the SID and Admin1 password is successfully set up to “swissbit”.

```

$ sudo ./sedutil-cli --initialsetup swissbit ↵
└─ /dev/nvme0

takeOwnership complete
Locking SP Activate Complete
LockingRangeo disabled
LockingRangeo set to RW
MBRDone set on
MBRDone set on
MBREnable set on
Initial setup of TPer complete on /dev/nvme0

```

After the initial setup, the password can still be changed with the command if required (only an example of setting up the SID password is given below; the same applies to the Admin1 password):

```

$ sudo ./sedutil-cli --setsidpassword swissbit ↵
└─ newPW /dev/nvmeo1

```

Now, the new SID password “newPW” has been set.

Note: The SID and Admin1 passwords don't have to be identical, but it makes things easier.

3.4 Enable the locking range

As the encryption has been initialized and the passwords are now successfully set and modified, you can enable the global range with the command --enablelockingrange and the Admin1 password.

```

$ sudo ./sedutil-cli --enablelockingrange 0 ↵
└─ newPW /dev/nvmeo

```

```

method status code NOT\_AUTHORIZED
Session start failed rc = 1
One or more header fields have 0 length
EndSession Failed

```

As shown above, an error occurs when trying to enable a locking range on the drive. The error message NOT_AUTHORIZED indicates that the password provided is probably incorrect. If you ignore the error message and repeat the command a few times, another error message as below may occur:

```

$ sudo ./sedutil-cli --enablelockingrange 0 ↵
└─ newPW /dev/nvmeo

```

```
method status code AUTHORITY_LOCKED_OUT
Session start failed rc = 18
One or more header fields have 0 length
EndSession Failed
```

The error `AUTHORITY_LOCKED_OUT` indicates that the SSD drive is being locked out from performing this operation. SED (Self-Encrypting Drive) security mechanisms will lock the drive out temporary after several failed attempts. In this case, a power cycle is required to unlock the SSD drive.

The root cause of these errors is that the wrong password "newPW" has been entered. After the initial set up, SID and Admin1 password is set up to "swissbit". Afterwards, the SID password was modified to "newPW". But there is no modification to the Admin1 password. Therefore, the Admin1 password for the command below to enable the locking range should be "swissbit" instead of "newPW".

```
$ sudo ./sedutil-cli --enablelockingrange 0 2
└─┬ swissbit /dev/nvmeo
```

```
LockingRange0 enabled ReadLocking,WriteLocking
```

Before setting up any locking ranges, you can use the command `--listlockingranges` to check all the ranges supported and their status. As demonstrated below, except for the global range (range 0), there are additional 8 ranges supported.

```
$ sudo ./sedutil-cli --listlockingranges swissbit 2
└─┬ /dev/nvmeo
```

```
Locking Range Configuration for /dev/nvmeo
LR0 Begin 0 for 0
    RLKEna = Y WLKEna = Y RLocked = N 2
    └─┬ WLocked = N
LR1 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
LR2 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
LR3 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
LR4 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
LR5 Begin 0 for 0
```

```
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
LR6 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
LR7 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
LR8 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = 2
    └─┬ N WLocked = N
```

3.5 Set up the locking range

Then you can set up a specific block number of a certain range using the command `--setuplockingrange`. Afterwards, you can configure the access permissions (Read/Write, Read-Only, or Locked) for the specific locking range.

```
$ sudo ./sedutil-cli --setuplockingrange 8 0 2
└─┬ 1000 swissbit /dev/nvmeo
```

```
LockingRange8 reKeyed
LockingRange8 starting block 0 for 1000 blocks 2
└─┬ configured as unlocked range
```

```
$ sudo ./sedutil-cli --setlockingrange 8 RO 2
└─┬ swissbit /dev/nvmeo
```

```
LockingRange8 set to RO
```

Now, the Locking range 8 was set to Read-Only. To make it work properly, you still need to get the write and read locks enabled (`RLKEna = Y` and `WLKEna = Y`) using the command `--enablelockingrange`.

```
$ sudo ./sedutil-cli --enablelockingrange 8 2
└─┬ swissbit /dev/nvmeo
```

```
LockingRange8 enabled ReadLocking,WriteLocking
```

3.6 Test the locking range

You can check if the desired access permission (Read-Only) is correctly set up for this locking range using the command `--listlockingranges` and verify it by writing something to the locked block areas.

```
$ sudo ./sedutil-cli --listlockingranges swissbit >
└ /dev/nvmeo
```

```
Locking Range Configuration for /dev/nvmeo
LR0 Begin 0 for 0
    RLKEna = Y WLKEna = Y RLocked = N >
    └ WLocked = N
LR1 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = >
    └ N WLocked = N
LR2 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = >
    └ N WLocked = N
LR3 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = >
    └ N WLocked = N
LR4 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = >
    └ N WLocked = N
LR5 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = >
    └ N WLocked = N
LR6 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = >
    └ N WLocked = N
LR7 Begin 0 for 0
    RLKEna = N WLKEna = N RLocked = >
    └ N WLocked = N
LR8 Begin 0 for 1000
    RLKEna = Y WLKEna = Y RLocked = N >
    └ WLocked = Y
```

```
$ sudo dd if=/dev/zero of=/dev/nvmeo1 >
└ count=1000 bs=512 status=progress
```

```
1000+0 records in
1000+0 records out
512000 bytes (512 kB, 500 KiB) copied, >
└ 0.00334352 s, 153 MB/s
```

The locked ranges can be written properly. It seems like locking range is not enforced properly. However, it should be noted that the above write operation is written to the OS cache and not directly to the disk. To make the test convincing, you need to bypass the OS cache (write directly to disk).

```
$ sudo dd if=/dev/zero of=/dev/nvmeo1 >
└ count=1000 bs=512 status=progress >
└ oflag=direct
```

```
dd: error writing '/dev/nvmeo1': No data >
└ available
```

```
1+0 records in
0+0 records out
0 bytes copied, 0.000657834 s, 0.0 kB/s
```

3.7 Reset the drive to Default

If you have forgotten the password, you can still reset the drive to its factory settings so that it can be set up again as described in the steps above. However, this will ERASE ALL DATA on the drive.

Reset the drive with the following command and the PSID (a 32-character password) key printed on the drive label.

```
$ sudo ./sedutil-cli -->
└ yesireallywanttoERASEALLmydatausingthePSID >
└ PSID /dev/nvmeo1
```

If the reset was successful, you'll receive the message "revertTper completed successfully". The drive is now in its factory default state, but all previous data has been deleted.

If you receive the message "NOT_AUTHORIZED", you may have entered the PSID incorrectly. Try again with the correct PSID.

NOTE: The PSID is not available in any other location, and it cannot be determined electronically from the SED itself. As such, the drive label needs to be protected during the SED's service life.

4 Summary

This document introduces how to configure encryption on a Swissbit PCIe NVMe SSD like N2000 m.2 SED Opal-compliant SSD using the tool SEDutil. It explains basic concepts and commands about how to take ownership of the drive, encrypt the data, and reset it to its default settings.

CONTACT US

Headquarters	Swissbit AG Industriestrasse 4 9552 Bronschhofen Switzerland	Tel. +41 71 913 03 03 sales@swissbit.com
Germany (Berlin)	Swissbit Germany AG Bitterfelder Strasse 22 12681 Berlin Germany	Tel. +49 30 936 954 0 sales@swissbit.com
Germany (Munich)	Swissbit Germany AG Leuchtenbergring 3 81677 Munich Germany	Tel. +49 30 936 954 400 sales@swissbit.com
North and South America	Swissbit NA Inc. 238 Littleton Road, Suite 202B Westford, MA 01886 USA	Tel. +1 978-490-3252 salesna@swissbit.com
Japan	Swissbit Japan Co., Ltd. CONCIERIA Tower West 2F 6-20-7 Nishishinjuku Shinjuku City, Tokyo 160-0023 Japan	Tel. +81 3 6258 0521 sales-japan@swissbit.com
Taiwan	Swissbit Taiwan 12 F.-9, No. 268, Liancheng Rd. Zhonghe District New Taipei City 235603 Taiwan, R.O.C.	Tel. +886 912 059 197 salesasia@swissbit.com
China	Swissbit China	Tel. +886 958 922 333 salesasia@swissbit.com

Disclaimer:

The information in this document is subject to change without notice. Swissbit AG ("SWISSBIT") assumes no responsibility for any errors or omissions that may appear in this document, and disclaims responsibility for any consequences resulting from the use of the information set forth herein. SWISSBIT makes no commitments to update or to keep current information contained in this document. The products listed in this document are not suitable for use in applications such as, but not limited to, aircraft control systems, aerospace equipment, submarine cables, nuclear reactor control systems and life support systems. Moreover, SWISSBIT does not recommend or approve the use of any of its products in life support devices or systems or in any application where failure could result in injury or death. If a customer wishes to use SWISSBIT products in applications not intended by SWISSBIT, said customer must contact an authorized SWISSBIT representative to determine SWISSBIT willingness to support a given application. The information set forth in this document does not convey any license under the copyrights, patent rights, trademarks or other intellectual property rights claimed and owned by SWISSBIT.

ALL PRODUCTS SOLD BY SWISSBIT ARE COVERED BY THE PROVISIONS APPEARING IN SWISSBIT'S TERMS AND CONDITIONS OF SALE ONLY, INCLUDING THE LIMITATIONS OF LIABILITY, WARRANTY AND INFRINGEMENT PROVISIONS. SWISSBIT MAKES NO WARRANTIES OF ANY KIND, EXPRESS, STATUTORY, IMPLIED OR OTHERWISE, REGARDING INFORMATION SET FORTH HEREIN OR REGARDING THE FREEDOM OF THE DESCRIBED PRODUCTS FROM INTELLECTUAL PROPERTY INFRINGEMENT, AND EXPRESSLY DISCLAIMS ANY SUCH WARRANTIES INCLUDING WITHOUT LIMITATION ANY EXPRESS, STATUTORY OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2025 SWISSBIT AG