Step-by-Step instructions to implement TCG OPAL SSC-based SED

This application note shows the step-by-step instructions to implement TCG OPAL SSC-based SED. Before implementation it is necessary to prepare Windows 10 Preboot Authentication (PBA). There are many alternative tools to create Windows 10 PBA such as key management software vendor WinMagic and McAfee. You also get the open source tool SEDutil and follow the procedure " How to use SEDutil for Windows 10 Preboot Authentication" to prepare boot settings in advance.

PBA boot

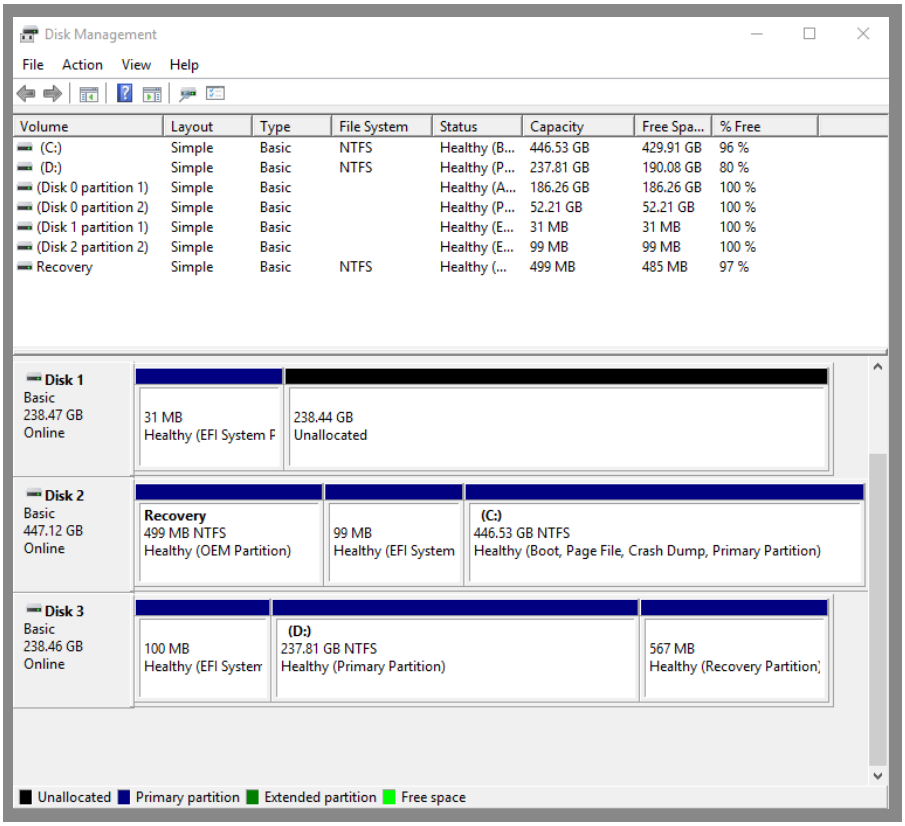
- When PBA boot setting is ready, reboot system and show the following prompt:



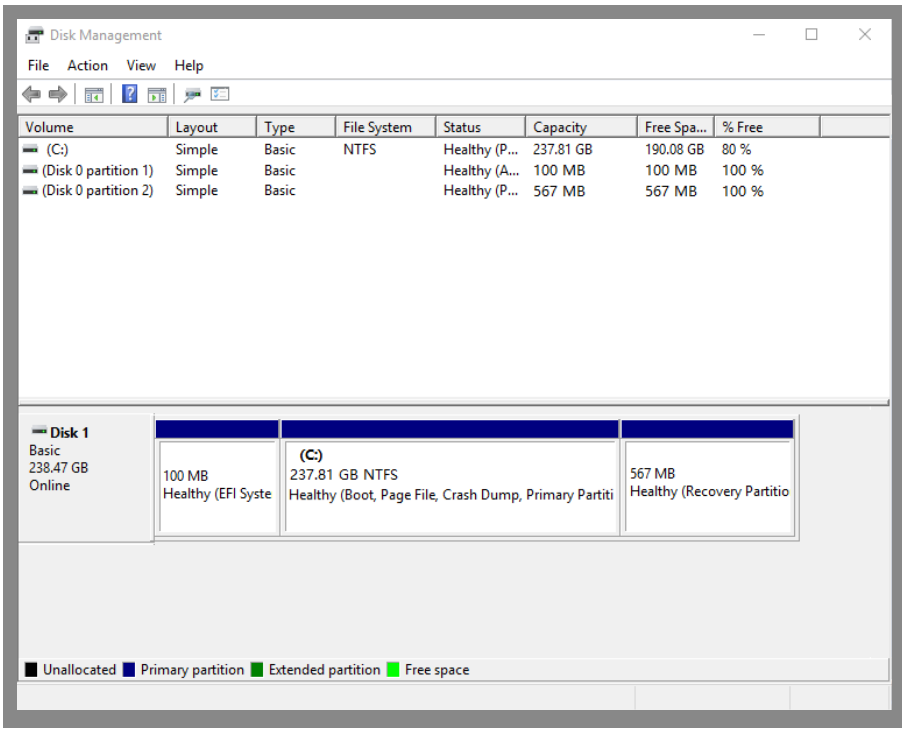
- Input "password'" , then login into console
- Input ID name "root" to login then input command "reboot" for warm reboot to pass Boot Authorization



- After finish warm boot-up and prompt password input, just press ENTER key to enter Windows 10 OS
- If SED is set up as Data Drive, then Windows system will show this SED drive as Non-partition drive as following.



- If SED is set up Boot Drive, system can show the normal partition via PBA boot.



Used case

- Scan drive

```
>sedutil-cli --scan
Scanning for Opal compliant disks
\\.\PhysicalDrive0 No   SP256GIMDC355EV0                          S0509A0
\\.\PhysicalDrive1  2      SP256GISSD355SV0                            02J0TBDD
\\.\PhysicalDrive2 No
\\.\PhysicalDrive3  2      SP128GISSD305RW0                            R0822A
\\.\PhysicalDrive4 No
```

- "\\.\PhysicalDrive0" is not OPAL 2.0 supported
- "\\.\PhysicalDrive1" & "\\.\PhysicalDrive3" is OPAL 2.0 supported

- Initialize "\\.\PhysicalDrive3"

```
>sedutil-cli.exe --initialSetup debug \\.\PhysicalDrive3
SID password changed
takeOwnership complete
Locking SP Activate Complete
LockingRange0 disabled
LockingRange0 set to RW
MBRDone set on
MBREnable set on
Initial setup of TPer complete on \\.\PhysicalDrive3
```

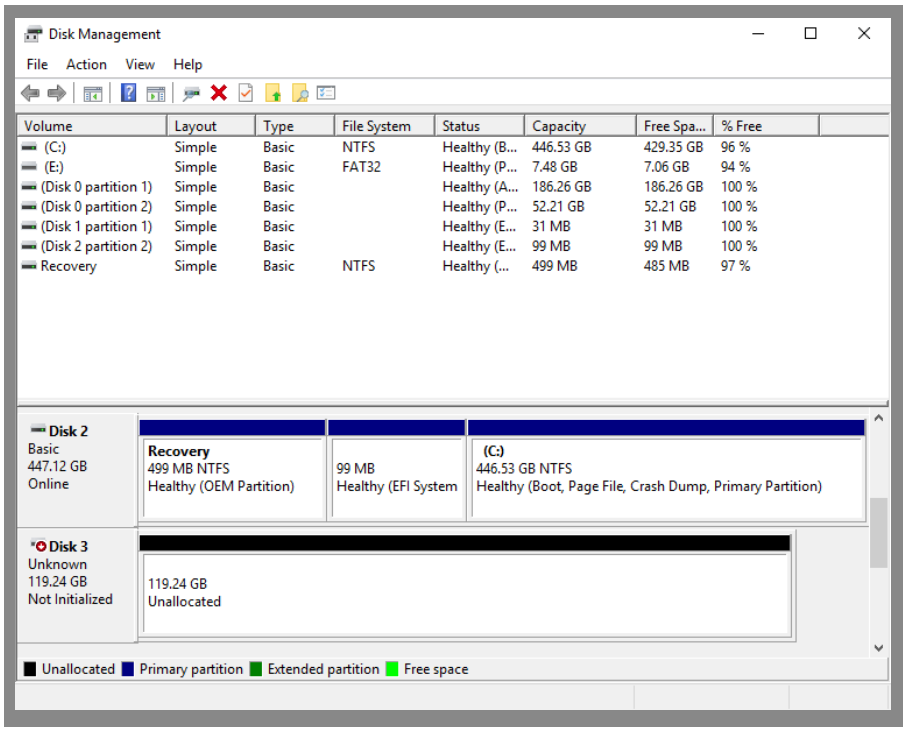
- Get information of "\\.\PhysicalDrive3"

```
>sedutil-cli.exe --query \\.\PhysicalDrive3
\\.\PhysicalDrive3 USB SP128GISSD305RW0                          R0822A    19012222020019
TPer function (0x0001)
      ACKNAK = N, ASYNC = N. BufferManagement = N, comIDManagement  = N, Streaming = Y, SYNC = Y
Locking function (0x0002)
      Locked = N, LockingEnabled = Y, LockingSupported = Y, MBRDone = Y, MBREnabled = Y,
      MBRAbsent = 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
Block SID Authentication function (0x0402)
      SID Blocked State = N, SID Value State = Y, Hardware Reset = N

TPer Properties:
  MaxComPacketSize = 32256  MaxResponseComPacketSize = 32256
  MaxPacketSize = 32236  MaxIndTokenSize = 32200  MaxPackets = 1
  MaxSubpackets = 1  MaxMethods = 1  MaxSessions = 1
  MaxAuthentications = 14  MaxTransactionLimit = 1  DefSessionTimeout = 0

Host Properties:
  MaxComPacketSize = 2048  MaxPacketSize = 2028
  MaxIndTokenSize = 1992  MaxPackets = 1  MaxSubpackets = 1
  MaxMethods = 1
```

- Attached SED to Windows 10 and checked via disk management , the show “unknown partition” as follows.



- When LockingEnable=Y, all of data of SED will be erased if execute command “revertTPer”

PSID Revert

The PSID is a 32 character password that can be used to prove you have physical access to the drive. It is printed on the drive label per request. The PSID revert function is useful if a third-party application or your OS has locked your drive and you are no longer able to access it because of some failure. It allows you to regain the use of the drive but all of the data on the drive will be erased.

```
>sedutil-cli.exe --yesIreallywanttoERASEALLmydatausingthePSID <32CharactersPSID> \\.\PhysicalDrive3

revertTper completed successfully
```

Remove OPAL function

- If you want to keep the data protected by the global locking range then you should perform a the Remove OPAL procedure if you have the Admin1 password

- Change LockingEnable=N

```
>sedutil-cli --revertNoErase debug \\.\PhysicalDrive3
Revert LockingSP complete
```

- Check status of LockingEnable and Remove OPAL

```
>sedutil-cli.exe --query \\.\PhysicalDrive3
\\.\PhysicalDrive3 USB SP128GISSD305RW0                          R0822A   19012222020019
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,
    MBRAbsent = 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
Block SID Authentication function (0x0402)
    SID Blocked State = N, SID Value State = Y, Hardware Reset = N

TPer Properties:
  MaxComPacketSize = 32256  MaxResponseComPacketSize = 32256
  MaxPacketSize = 32236  MaxIndTokenSize = 32200  MaxPackets = 1
  MaxSubpackets = 1  MaxMethods = 1  MaxSessions = 1
  MaxAuthentications = 14  MaxTransactionLimit = 1  DefSessionTimeout = 0

Host Properties:
  MaxComPacketSize = 2048  MaxPacketSize = 2028
  MaxIndTokenSize = 1992  MaxPackets = 1  MaxSubpackets = 1
  MaxMethods = 1


>sedutil-cli --revertTPer debug \\.\PhysicalDrive3
revertTper completed successfully
```

* Information might be changed or updated without notice.

All trademarks, brands and names are the property of their respective owners.
©2021 SILICON POWER Computer & Communications, Inc., All Rights Reserved.