Intel® Virtual RAID on CPU (Intel® VROC) Self-Encrypting Drive Feature

User Guide

Revision 1.1

March 2024

Document Number:759299

Contents

Figures

Revision History

Revision Number	Description	Date
1.0	• Initial release.	February 2023
1.1	• Added re-key and limitation.	March 2024

§§

1 Introduction

This document describes the operations of the Intel® Virtual RAID on CPU (Intel® VROC) Self-Encrypting Drive feature for the Intel® Virtual RAID on CPU (Intel® VROC) products based on Intel® Xeon® Scalable Generation 3, and higher, platforms.

1.1 SED and OPAL Overview

1. Self-Encrypting Drive (SED) is a Storage Device that integrates encryption of user data at rest, all user data written to the Storage Device is encrypted by specialized hardware implemented inside the Storage Device controller. The data is decrypted as it is read.
2. OPAL is a specification provides a scalable infrastructure for managing encryption of user data in a Storage Device, as well as extensibility to enable features beyond "data at rest protection".

§§

2 Intel® VROC SED Functions

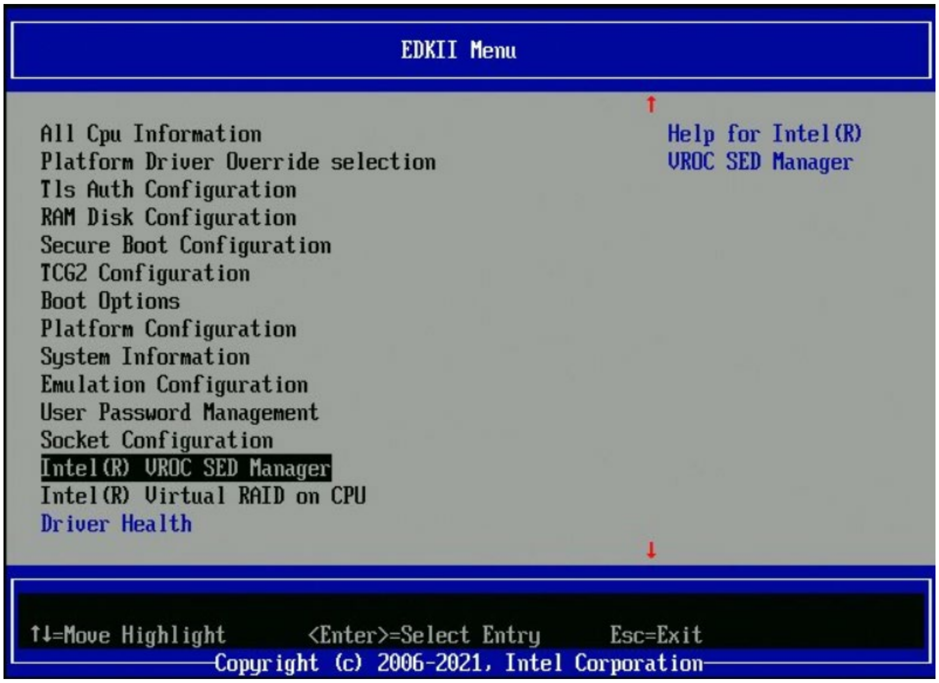
Configuration:

1. HW: Intel® Whitley CRB
2. BIOS: Whitley_ICX BKC BIOS
3. Intel® VROC SED UEFI driver: Intel VROC SED UEFI drivers need to be included in BIOS. Please contact Intel VROC AE for VROC SED UEFI drivers.
4. NVMe SSD: OPAL drives (VROC SED can be only enabled on drives supported OPAL storage specification).

2.1 How to Enable Intel® VROC SED in BIOS

Go to EDKII Menu → Socket Configuration → IIO Configuration → Intel VMD technology then enable ports where OPAL drives are connected. After system reboot, you should be able to see Intel® VROC SED manager in BIOS.

Figure 2-1. EDKII Menu



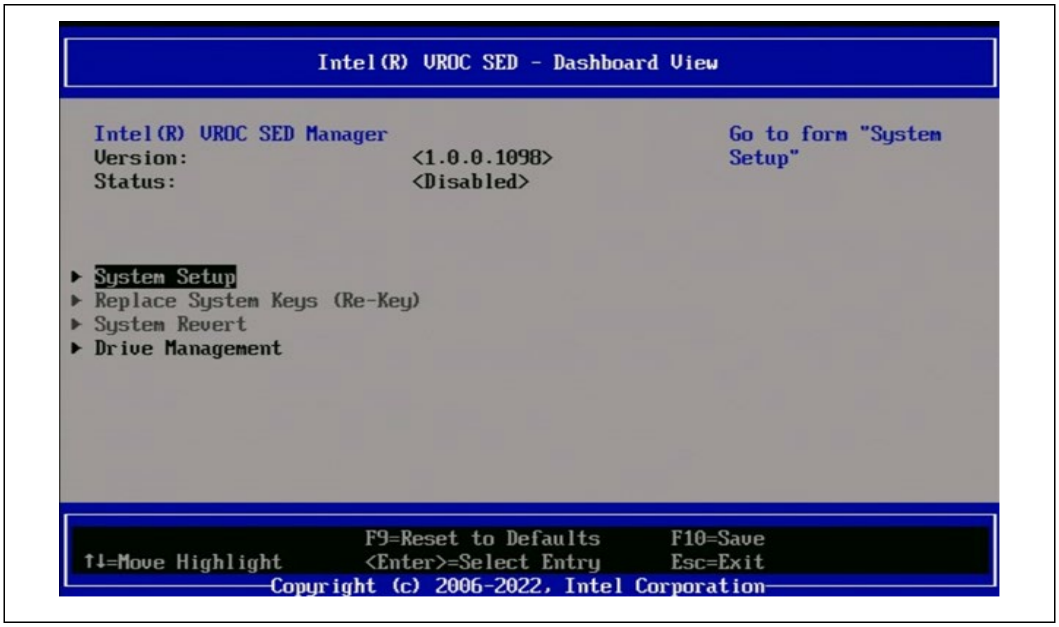
```
                         EDKII Menu

  All Cpu Information                              Help for Intel(R)
  Platform Driver Override selection               VROC SED Manager
  Tls Auth Configuration
  RAM Disk Configuration
  Secure Boot Configuration
  TCG2 Configuration
  Boot Options
  Platform Configuration
  System Information
  Emulation Configuration
  User Password Management
  Socket Configuration
  Intel(R) VROC SED Manager
  Intel(R) Virtual RAID on CPU
  Driver Health

 ↑↓=Move Highlight       <Enter>=Select Entry       Esc=Exit
            Copyright (c) 2006-2021, Intel Corporation
```

NOTE: If no NVMe driver is present in system, Intel® VROC SED manager and Intel® Virtual RAID on CPU HII is not displayed.

2.2 Enable Self-Encrypting

1. When system boots up, go to BIOS Menu, find Intel® VROC SED Manager then enter. Enter SED manager, the following screen appears.

Figure 2-2. Dashboard View



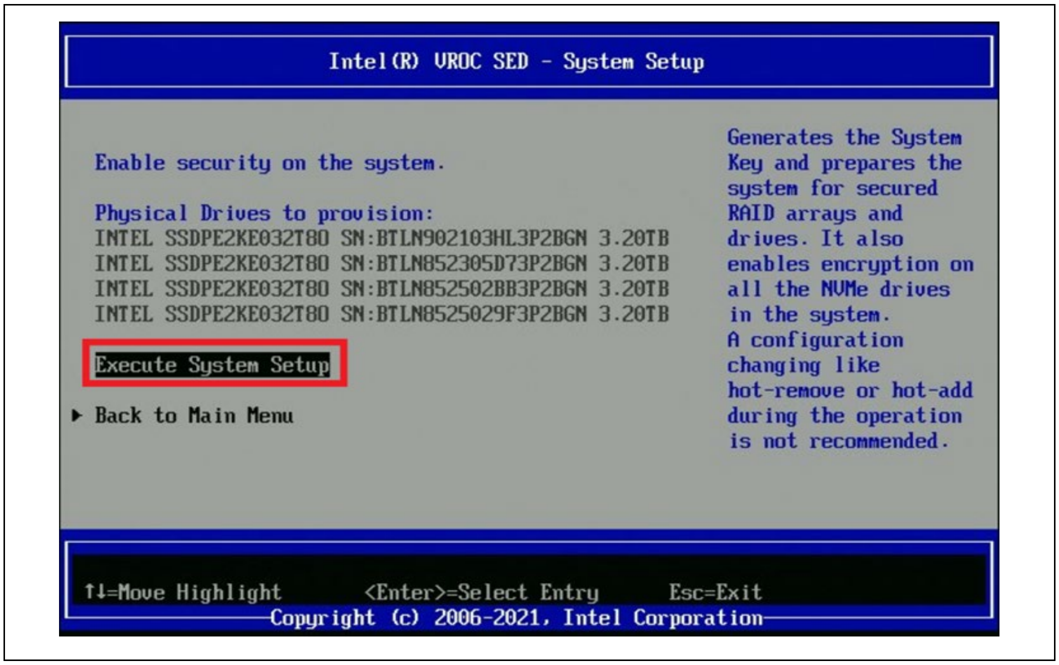
```
                    Intel(R) VROC SED - Dashboard View

  Intel(R) VROC SED Manager                         Go to form "System
  Version:                  <1.0.0.1098>            Setup"
  Status:                   <Disabled>


▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management


                         F9=Reset to Defaults       F10=Save
 ↑↓=Move Highlight       <Enter>=Select Entry       Esc=Exit
                Copyright (c) 2006-2022, Intel Corporation
```

NOTE: If no NVMe driver is present in system, Intel® VROC SED manager and Intel® Virtual RAID on CPU HII is not displayed.

In system setup menu, the eligible drives for provision are displayed.

2. To Execute System Setup for enable encrypting:

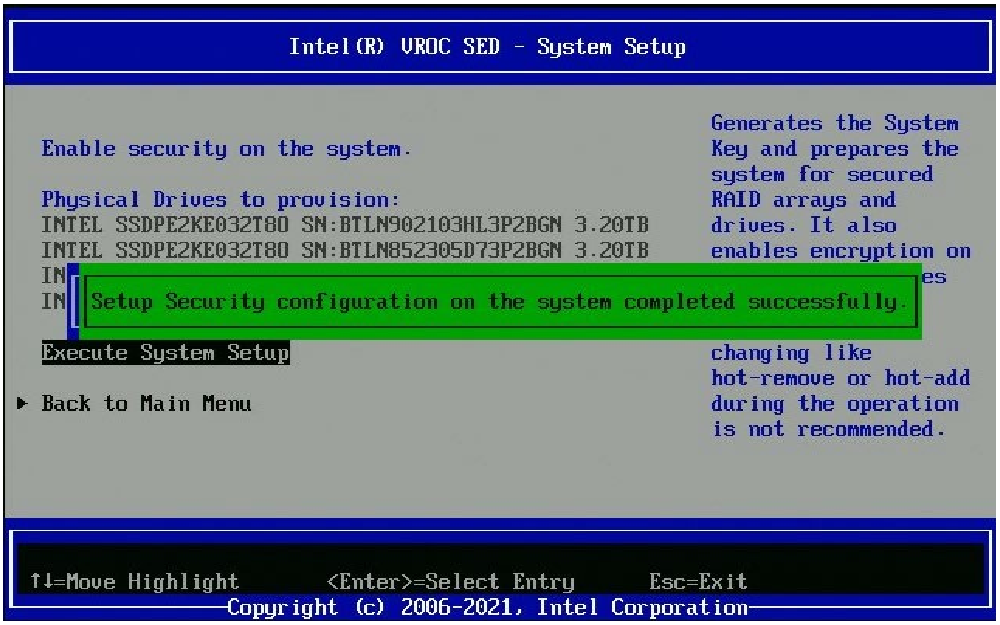
Figure 2-3. System Setup



```
                    Intel(R) VROC SED - System Setup

                                                    Generates the System
  Enable security on the system.                    Key and prepares the
                                                    system for secured
  Physical Drives to provision:                     RAID arrays and
  INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB drives. It also
  INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB enables encryption on
  INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB all the NVMe drives
  INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB in the system.
                                                    A configuration
  Execute System Setup                              changing like
                                                    hot-remove or hot-add
▶ Back to Main Menu                                 during the operation
                                                    is not recommended.


 ↑↓=Move Highlight       <Enter>=Select Entry       Esc=Exit
                Copyright (c) 2006-2021, Intel Corporation
```

When successful, the following screen appears.

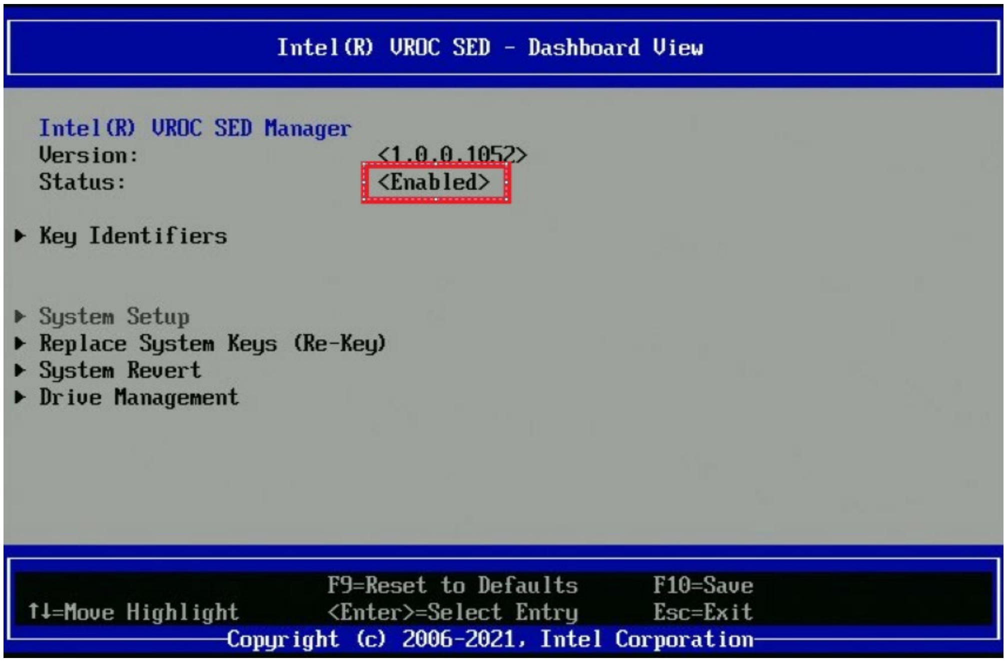
Figure 2-4. System Completed Screen



```
                 Intel(R) VROC SED - System Setup

                                                 Generates the System
 Enable security on the system.                  Key and prepares the
                                                 system for secured
 Physical Drives to provision:                   RAID arrays and
 INTEL SSDPE2KE032T8O SN:BTLN902103HL3P2BGN 3.20TB drives. It also
 INTEL SSDPE2KE032T8O SN:BTLN852305D73P2BGN 3.20TB enables encryption on
 IN                                                es
 IN  Setup Security configuration on the system completed successfully.

 Execute System Setup                            changing like
                                                 hot-remove or hot-add
▶ Back to Main Menu                              during the operation
                                                 is not recommended.

 ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2006-2021, Intel Corporation
```

3. Return to Dashboard View, the status is changed to "Enabled".

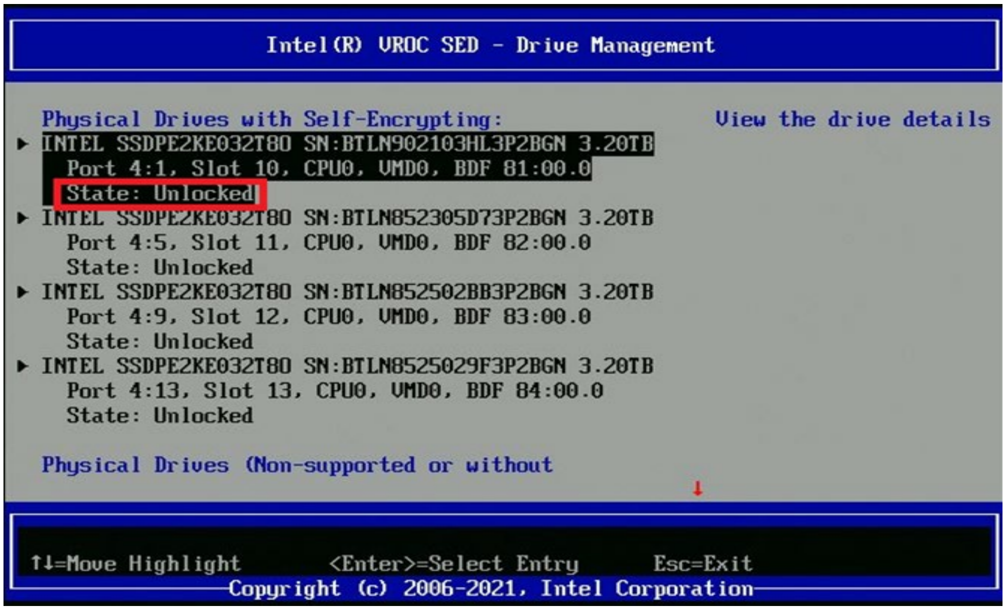
Figure 2-5. Dashboard View - Enabled



```
                 Intel(R) VROC SED - Dashboard View

 Intel(R) VROC SED Manager
 Version:                      <1.0.0.1052>
 Status:                       <Enabled>

▶ Key Identifiers


▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management



                         F9=Reset to Defaults      F10=Save
 ↑↓=Move Highlight       <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2006-2021, Intel Corporation
```

4. Check the physical drive state, it indicates the security state of the drive is unlocked in Drive Management menu.

Figure 2-6. Drive Management

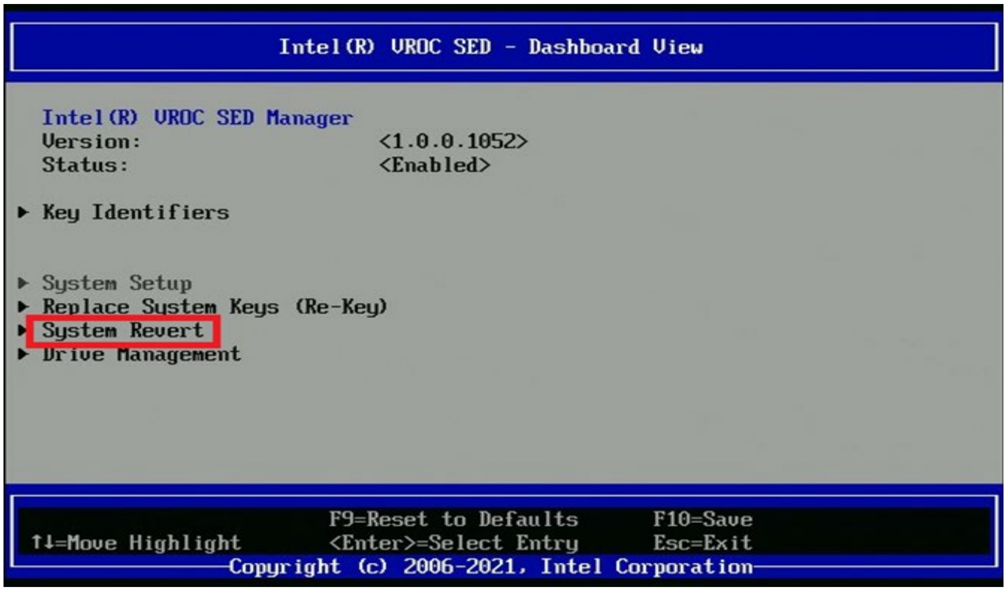


```
                 Intel(R) VROC SED - Drive Management

 Physical Drives with Self-Encrypting:                View the drive details
▶ INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB
   Port 4:1, Slot 10, CPU0, VMD0, BDF 81:00.0
   State: Unlocked
▶ INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
   Port 4:5, Slot 11, CPU0, VMD0, BDF 82:00.0
   State: Unlocked
▶ INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
   Port 4:9, Slot 12, CPU0, VMD0, BDF 83:00.0
   State: Unlocked
▶ INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB
   Port 4:13, Slot 13, CPU0, VMD0, BDF 84:00.0
   State: Unlocked

 Physical Drives (Non-supported or without
                                                        ↓

 ↑↓=Move Highlight        <Enter>=Select Entry       Esc=Exit
                  Copyright (c) 2006-2021, Intel Corporation
```

2.3 System Revert

1. When system boot up, go to BIOS Menu, find Intel® VROC SED Manager then enter System Revert. All secured drives are displayed.

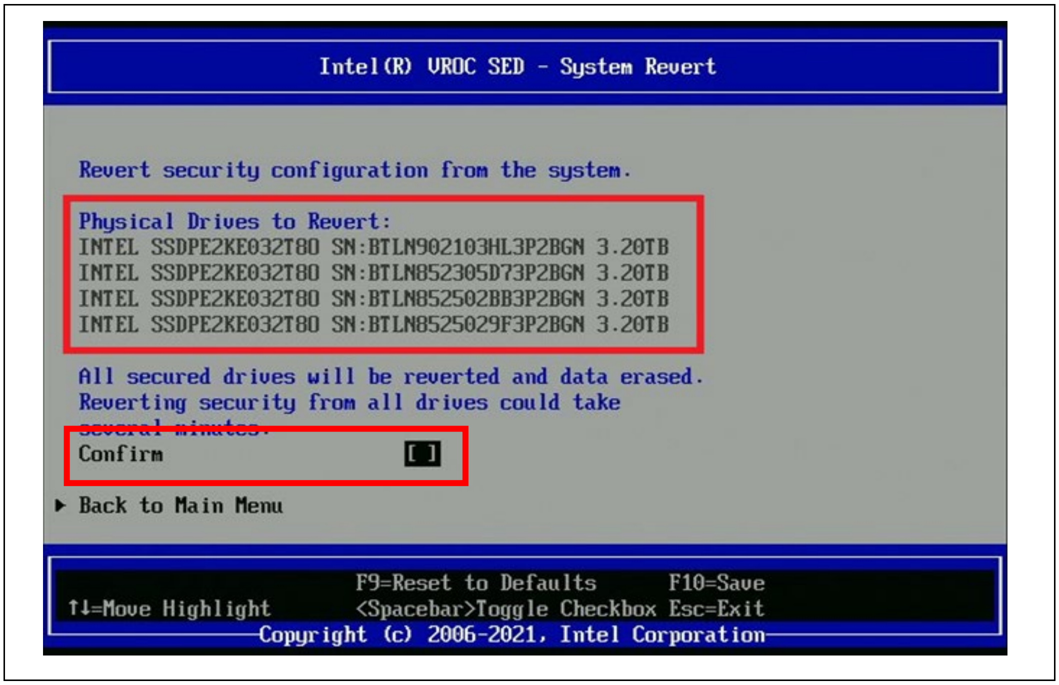
Figure 2-7. Dashboard View – System Revert



```
                 Intel(R) VROC SED - Dashboard View

 Intel(R) VROC SED Manager
 Version:                           <1.0.0.1052>
 Status:                            <Enabled>

▶ Key Identifiers


▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management



                          F9=Reset to Defaults       F10=Save
 ↑↓=Move Highlight        <Enter>=Select Entry       Esc=Exit
                  Copyright (c) 2006-2021, Intel Corporation
```

2. Check the Confirm Box.

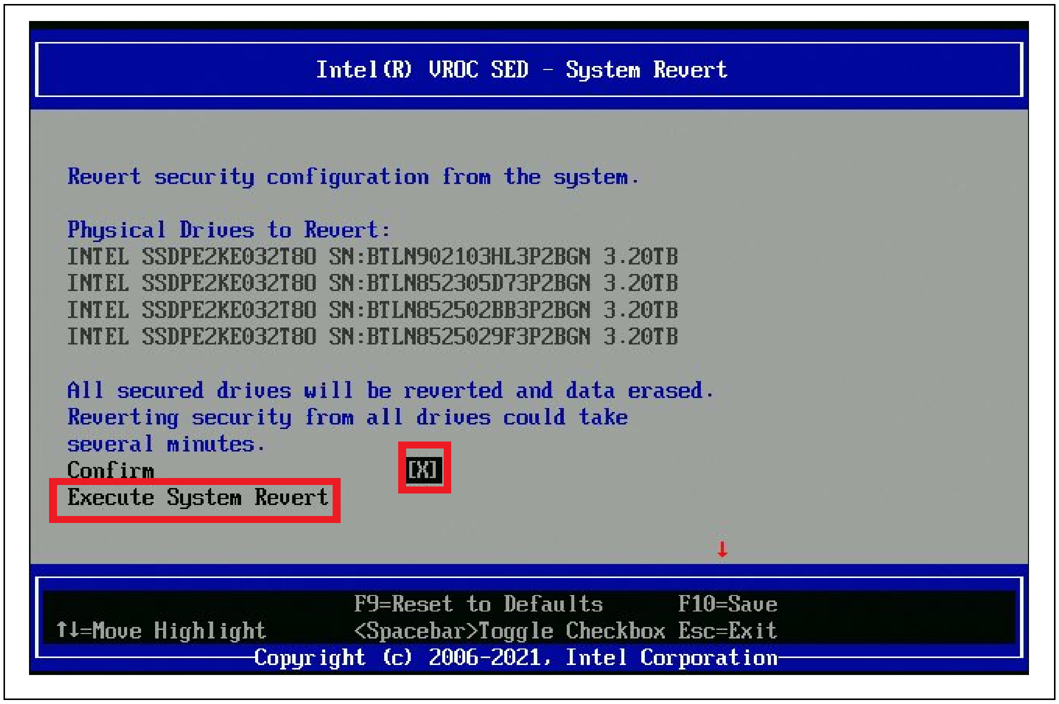
Figure 2-8. Dashboard View – System Revert Confirm Box



```
                Intel(R) VROC SED - System Revert

 Revert security configuration from the system.

 Physical Drives to Revert:
 INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB
 INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
 INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
 INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB

 All secured drives will be reverted and data erased.
 Reverting security from all drives could take
 several minutes.
 Confirm                            [ ]

▶ Back to Main Menu

                      F9=Reset to Defaults       F10=Save
↑↓=Move Highlight     <Spacebar>Toggle Checkbox  Esc=Exit
               Copyright (c) 2006-2021, Intel Corporation
```

3. Execute System Revert

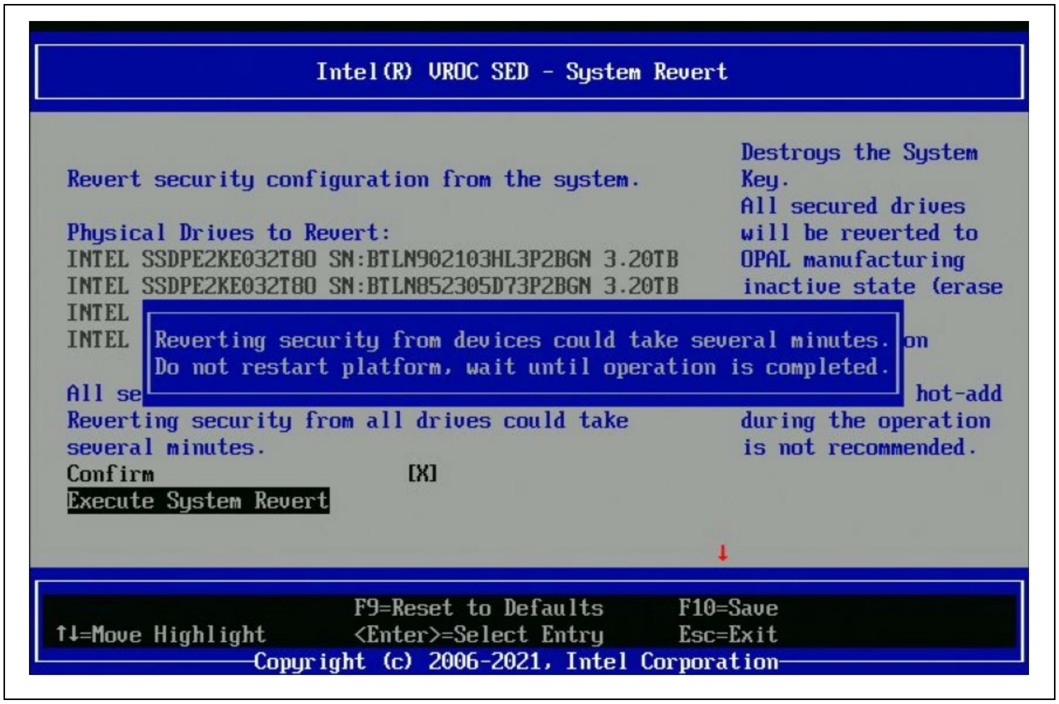
Figure 2-9. System Revert



```
                Intel(R) VROC SED - System Revert

 Revert security configuration from the system.

 Physical Drives to Revert:
 INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB
 INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
 INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
 INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB

 All secured drives will be reverted and data erased.
 Reverting security from all drives could take
 several minutes.
 Confirm                            [X]
 Execute System Revert

                                                   ↓
                      F9=Reset to Defaults       F10=Save
↑↓=Move Highlight     <Spacebar>Toggle Checkbox  Esc=Exit
               Copyright (c) 2006-2021, Intel Corporation
```

4. During the drive revert, do not restart the platform until the operation is completed.

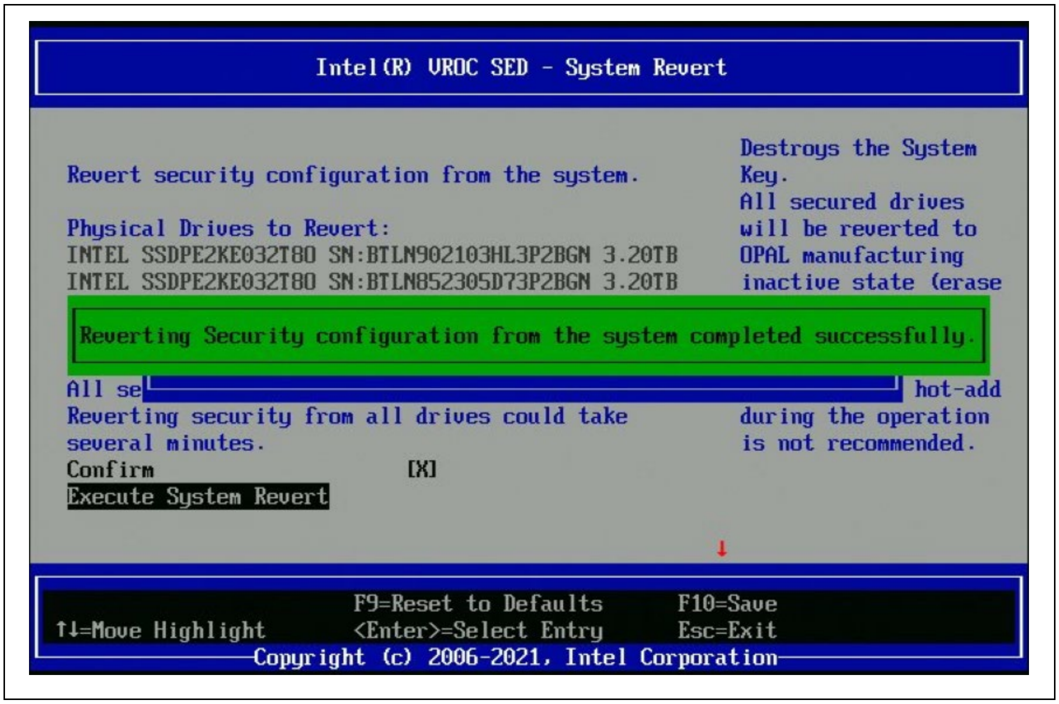
Figure 2-10. System Revert – Completed Message



```
                Intel(R) VROC SED - System Revert

                                                  Destroys the System
  Revert security configuration from the system.  Key.
                                                  All secured drives
  Physical Drives to Revert:                      will be reverted to
  INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB OPAL manufacturing
  INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB inactive state (erase
  INTEL
  INTEL |Reverting security from devices could take several minutes.|on
        |Do not restart platform, wait until operation is completed.|
  All se                                                     hot-add
  Reverting security from all drives could take   during the operation
  several minutes.                                is not recommended.
  Confirm                  [X]
  Execute System Revert

                    F9=Reset to Defaults      F10=Save
  ↑↓=Move Highlight <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2006-2021, Intel Corporation
```

5. After successful Revert, the following screen appears.

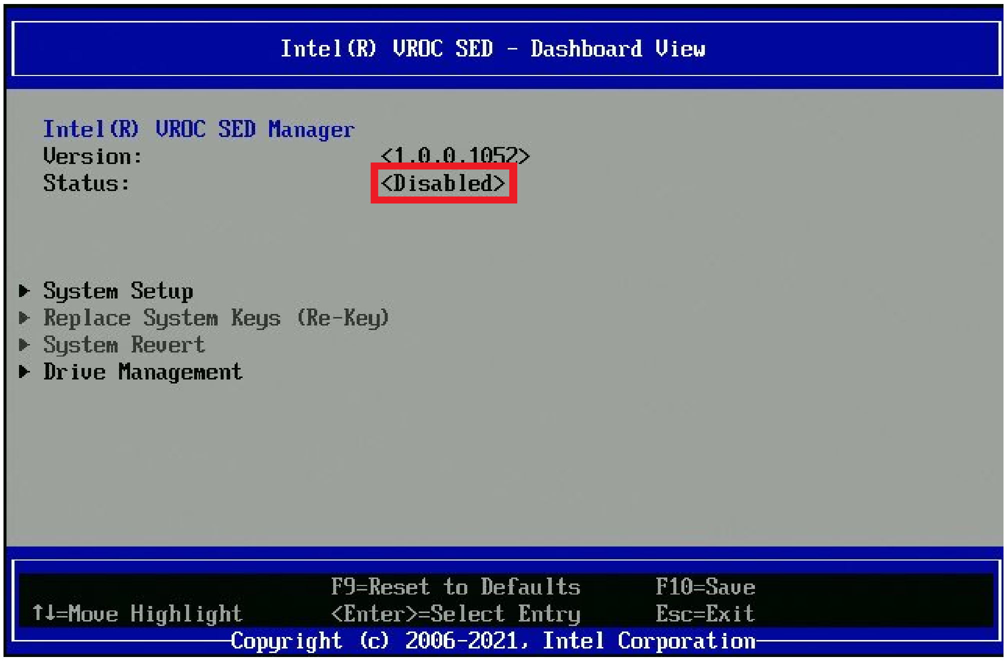
Figure 2-11. System Revert – Successfully Completed Message



```
                Intel(R) VROC SED - System Revert

                                                  Destroys the System
  Revert security configuration from the system.  Key.
                                                  All secured drives
  Physical Drives to Revert:                      will be reverted to
  INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB OPAL manufacturing
  INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB inactive state (erase

  |Reverting Security configuration from the system completed successfully.|

  All se                                                     hot-add
  Reverting security from all drives could take   during the operation
  several minutes.                                is not recommended.
  Confirm                  [X]
  Execute System Revert

                    F9=Reset to Defaults      F10=Save
  ↑↓=Move Highlight <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2006-2021, Intel Corporation
```

The Dashboard View changes to Disabled.

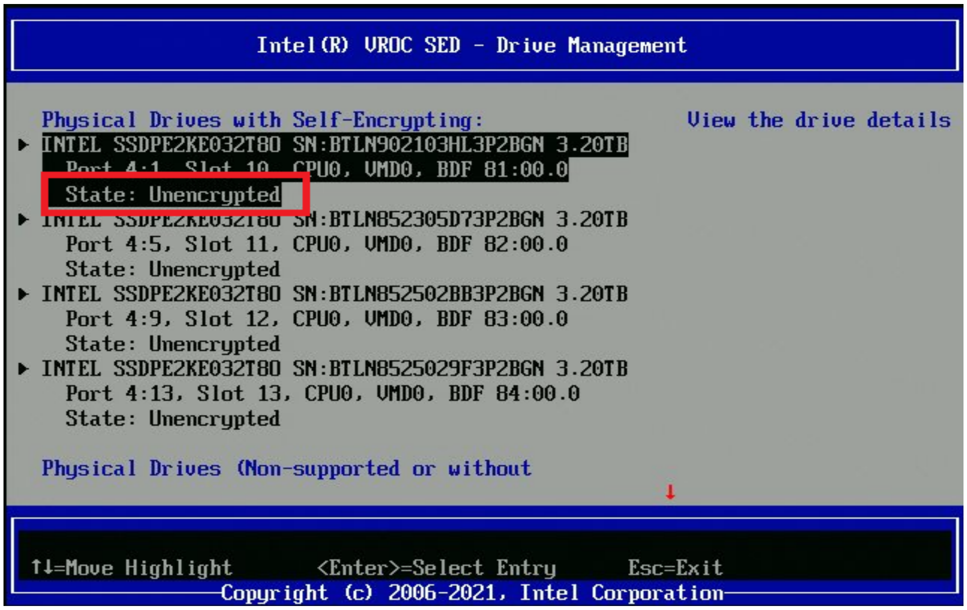
Figure 2-12. Dashboard View - Disabled



```
               Intel(R) VROC SED - Dashboard View

 Intel(R) VROC SED Manager
 Version:                    <1.0.0.1052>
 Status:                     <Disabled>


▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management


                        F9=Reset to Defaults      F10=Save
 ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit
          Copyright (c) 2006-2021, Intel Corporation
```

In Drive Management, the state drive is Not Provisioned.

Figure 2-13. Drive Management – Not Provisioned

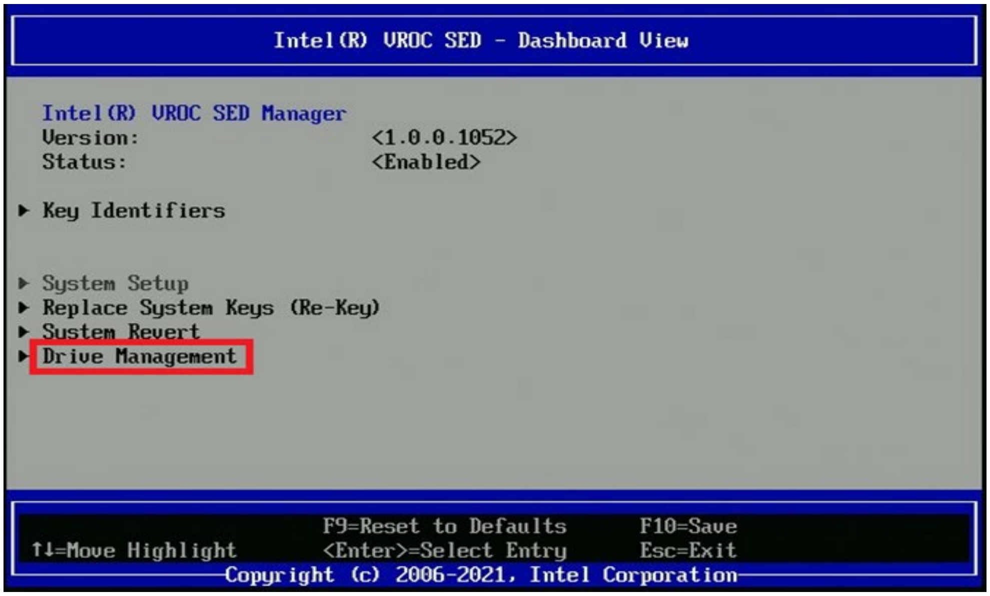


```
            Intel(R) VROC SED - Drive Management

 Physical Drives with Self-Encrypting:               View the drive details
▶ INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB
    Port 4:1, Slot 10, CPU0, VMD0, BDF 81:00.0
    State: Unencrypted
▶ INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
    Port 4:5, Slot 11, CPU0, VMD0, BDF 82:00.0
    State: Unencrypted
▶ INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
    Port 4:9, Slot 12, CPU0, VMD0, BDF 83:00.0
    State: Unencrypted
▶ INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB
    Port 4:13, Slot 13, CPU0, VMD0, BDF 84:00.0
    State: Unencrypted

 Physical Drives (Non-supported or without
                                               ↓

 ↑↓=Move Highlight       <Enter>=Select Entry      Esc=Exit
          Copyright (c) 2006-2021, Intel Corporation
```

2.4 Drive Revert

1. After system boot up, go to BIOS Menu, find Intel® VROC SED Manager then go to Drive Management.

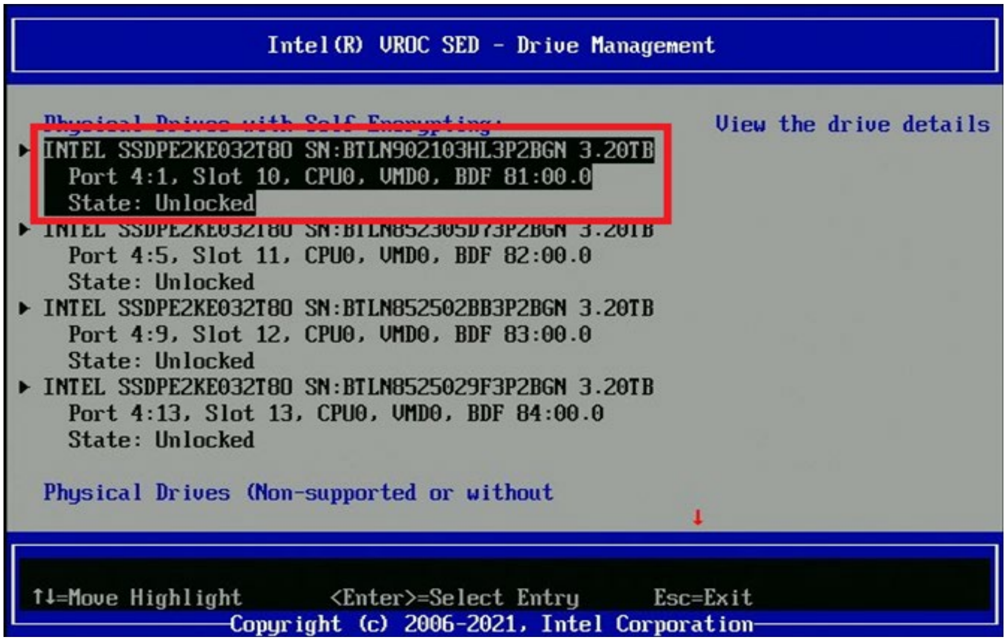
Figure 2-14. Dashboard View - Drive Management



```
                    Intel(R) VROC SED - Dashboard View

  Intel(R) VROC SED Manager
  Version:                       <1.0.0.1052>
  Status:                        <Enabled>

▶ Key Identifiers


▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management


                         F9=Reset to Defaults      F10=Save
 ↑↓=Move Highlight       <Enter>=Select Entry      Esc=Exit
                Copyright (c) 2006-2021, Intel Corporation
```

2. Select drive to disable self-encrypting and open it.

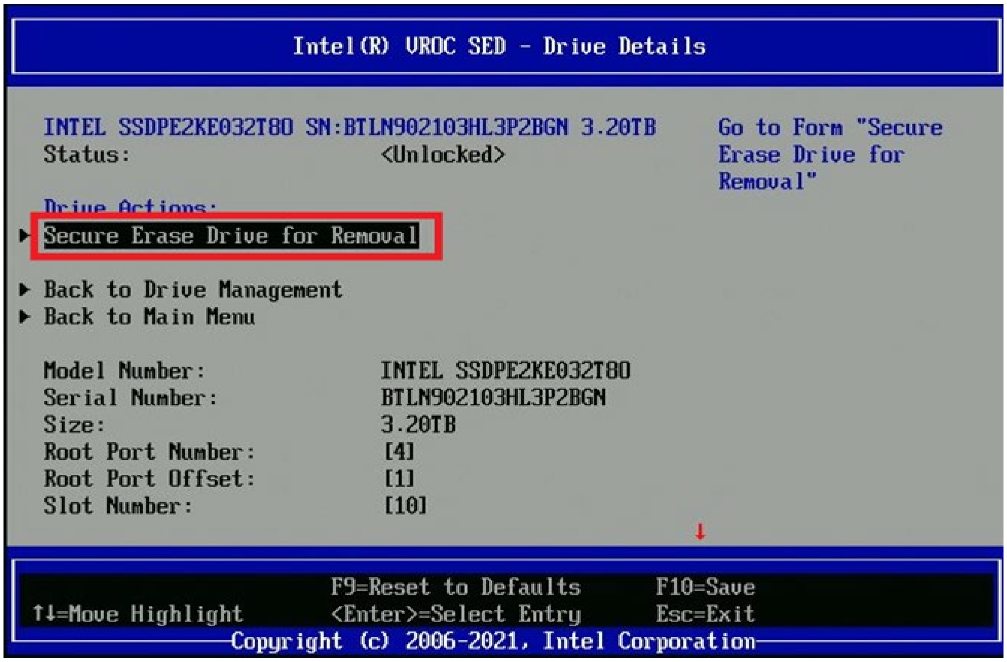
Figure 2-15. Drive Management



```
                    Intel(R) VROC SED - Drive Management

  Physical Drives with Self Encrypting:                    View the drive details
▶ INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB
    Port 4:1, Slot 10, CPU0, VMD0, BDF 81:00.0
    State: Unlocked
▶ INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
    Port 4:5, Slot 11, CPU0, VMD0, BDF 82:00.0
    State: Unlocked
▶ INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
    Port 4:9, Slot 12, CPU0, VMD0, BDF 83:00.0
    State: Unlocked
▶ INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB
    Port 4:13, Slot 13, CPU0, VMD0, BDF 84:00.0
    State: Unlocked

  Physical Drives (Non-supported or without
                                                      ↓

 ↑↓=Move Highlight        <Enter>=Select Entry       Esc=Exit
                Copyright (c) 2006-2021, Intel Corporation
```

3. Click Prepare drive for removal (Secure Erase)

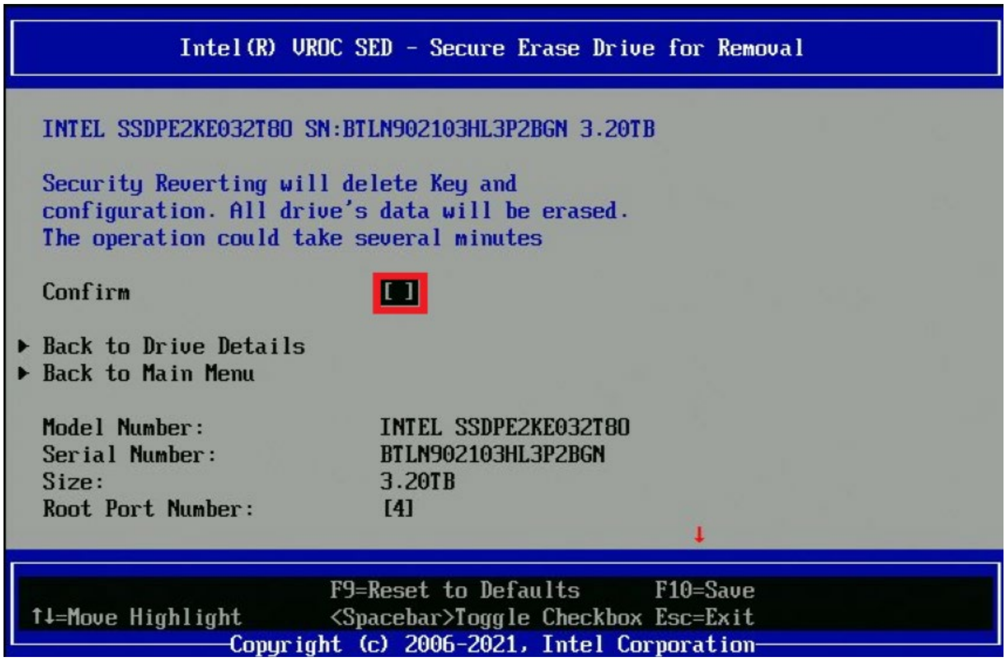
Figure 2-16. Drive Details



```
Intel(R) VROC SED - Drive Details

INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB     Go to Form "Secure
Status:                       <Unlocked>               Erase Drive for
                                                       Removal"
Drive Actions:
▶ Secure Erase Drive for Removal

▶ Back to Drive Management
▶ Back to Main Menu

Model Number:                 INTEL SSDPE2KE032T80
Serial Number:                BTLN902103HL3P2BGN
Size:                         3.20TB
Root Port Number:             [4]
Root Port Offset:             [1]
Slot Number:                  [10]

                        F9=Reset to Defaults       F10=Save
↑↓=Move Highlight       <Enter>=Select Entry       Esc=Exit
             Copyright (c) 2006-2021, Intel Corporation
```

4. Check the Confirm Box.

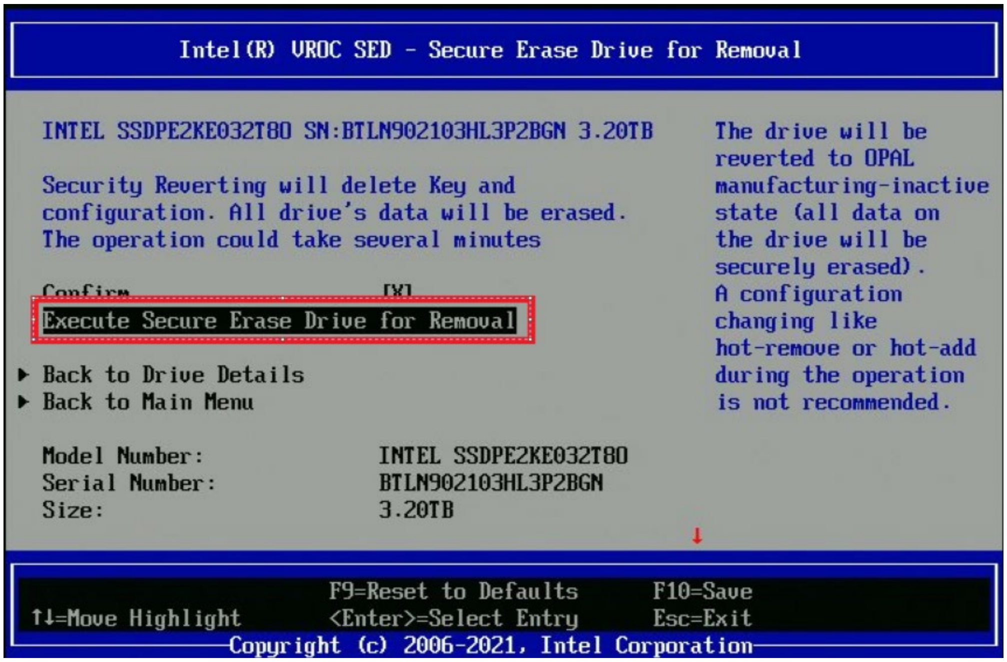
Figure 2-17. Secure Erase Drive for Removal – Confirm Box



```
Intel(R) VROC SED - Secure Erase Drive for Removal

INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB

Security Reverting will delete Key and
configuration. All drive's data will be erased.
The operation could take several minutes

Confirm                       [ ]

▶ Back to Drive Details
▶ Back to Main Menu

Model Number:                 INTEL SSDPE2KE032T80
Serial Number:                BTLN902103HL3P2BGN
Size:                         3.20TB
Root Port Number:             [4]

                        F9=Reset to Defaults       F10=Save
↑↓=Move Highlight       <Spacebar>Toggle Checkbox  Esc=Exit
             Copyright (c) 2006-2021, Intel Corporation
```

5. Execute Secure Erase - Prepare drive for removal.

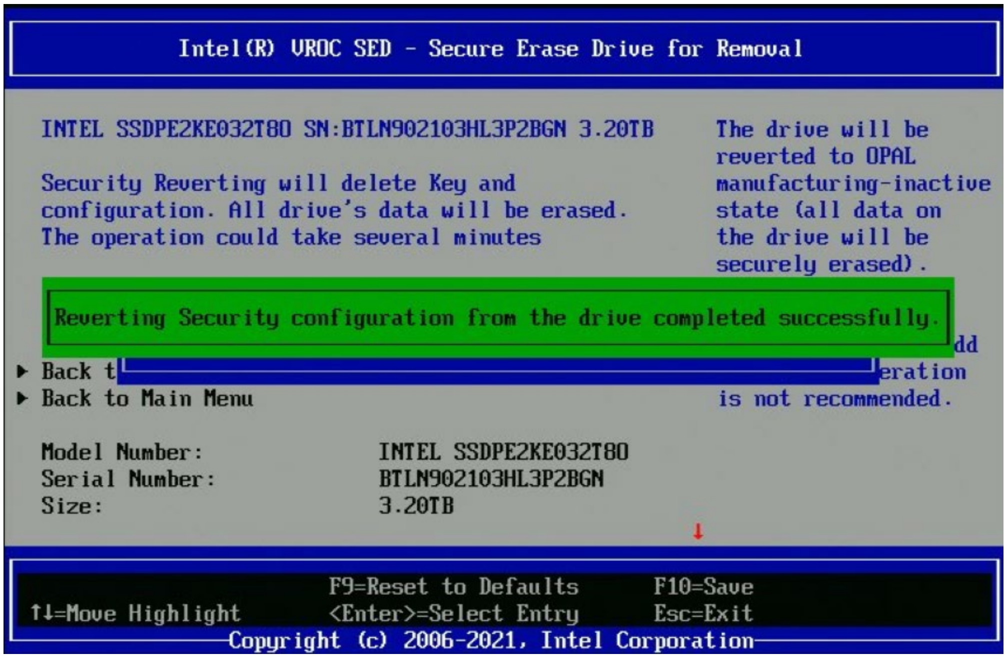
Figure 2-18. Secure Erase Drive for Removal



```
                 Intel(R) VROC SED - Secure Erase Drive for Removal

 INTEL SSDPE2KE032T8O SN:BTLN902103HL3P2BGN 3.20TB     The drive will be
                                                       reverted to OPAL
 Security Reverting will delete Key and                manufacturing-inactive
 configuration. All drive's data will be erased.       state (all data on
 The operation could take several minutes              the drive will be
                                                       securely erased).
 Confirm                    [X]                        A configuration
 Execute Secure Erase Drive for Removal                changing like
                                                       hot-remove or hot-add
▶ Back to Drive Details                                during the operation
▶ Back to Main Menu                                    is not recommended.

 Model Number:              INTEL SSDPE2KE032T8O
 Serial Number:             BTLN902103HL3P2BGN
 Size:                      3.20TB

                            F9=Reset to Defaults      F10=Save
 ↑↓=Move Highlight          <Enter>=Select Entry      Esc=Exit
                 Copyright (c) 2006-2021, Intel Corporation
```

After a successful erase, the following screen appears.

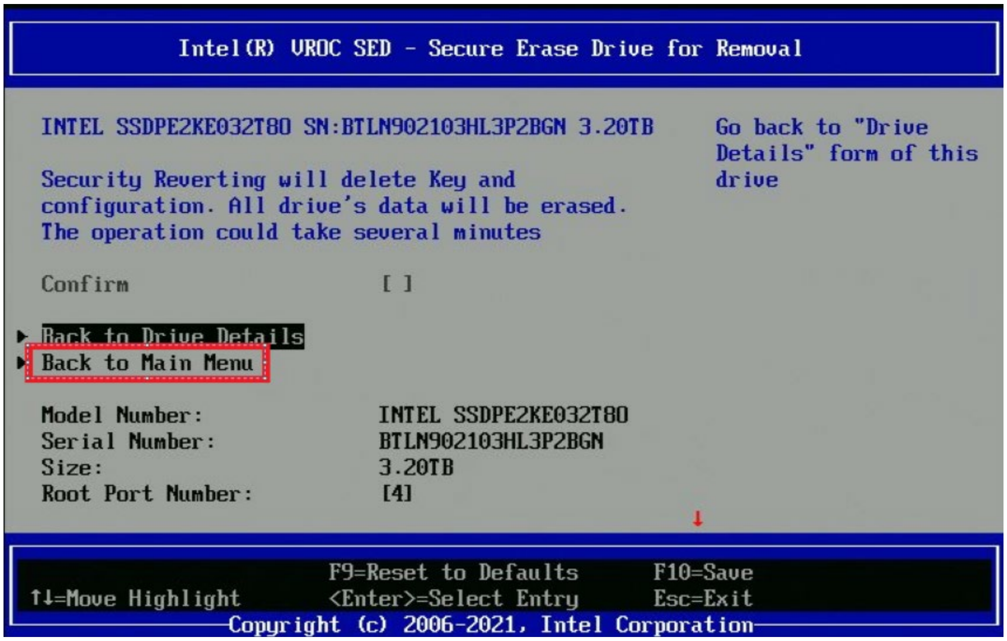
Figure 2-19. Secure Erase Drive for Removal– Completed Successfully Message



```
                 Intel(R) VROC SED - Secure Erase Drive for Removal

 INTEL SSDPE2KE032T8O SN:BTLN902103HL3P2BGN 3.20TB     The drive will be
                                                       reverted to OPAL
 Security Reverting will delete Key and                manufacturing-inactive
 configuration. All drive's data will be erased.       state (all data on
 The operation could take several minutes              the drive will be
                                                       securely erased).
 Reverting Security configuration from the drive completed successfully.
                                                                         dd
▶ Back t                                                          eration
▶ Back to Main Menu                                    is not recommended.

 Model Number:              INTEL SSDPE2KE032T8O
 Serial Number:             BTLN902103HL3P2BGN
 Size:                      3.20TB

                            F9=Reset to Defaults      F10=Save
 ↑↓=Move Highlight          <Enter>=Select Entry      Esc=Exit
                 Copyright (c) 2006-2021, Intel Corporation
```

6. Return to the Main Menu.

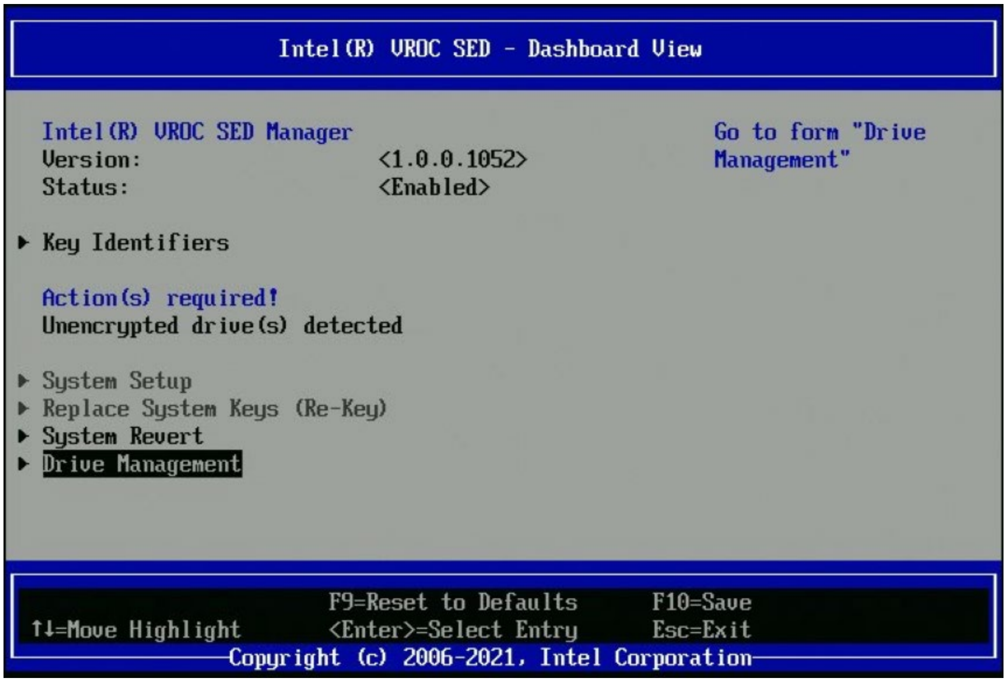
Figure 2-20. Secure Erase Drive for Removal– Back to Main Menu



```
Intel(R) VROC SED - Secure Erase Drive for Removal

INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB          Go back to "Drive
                                                           Details" form of this
Security Reverting will delete Key and                     drive
configuration. All drive's data will be erased.
The operation could take several minutes

Confirm                            [ ]

▶ Back to Drive Details
▶ Back to Main Menu

Model Number:                      INTEL SSDPE2KE032T80
Serial Number:                     BTLN902103HL3P2BGN
Size:                              3.20TB
Root Port Number:                  [4]

                          F9=Reset to Defaults      F10=Save
↑↓=Move Highlight         <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2006-2021, Intel Corporation
```

7. Select Drive Management.

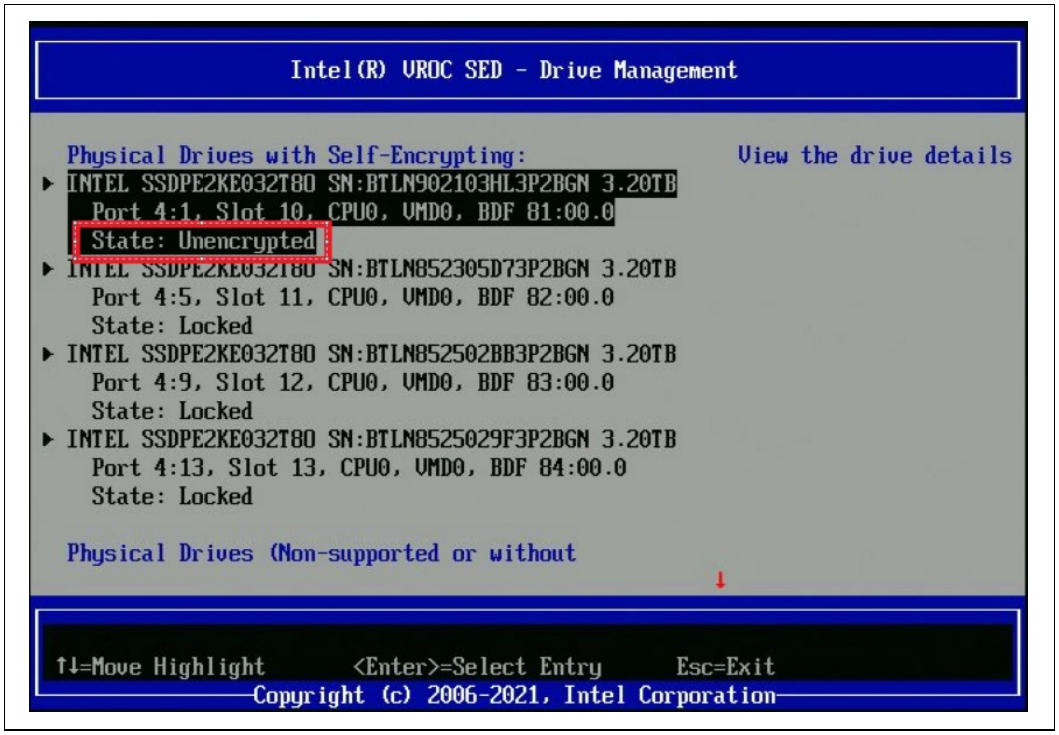
Figure 2-21. Dashboard View – Drive Management



```
Intel(R) VROC SED - Dashboard View

Intel(R) VROC SED Manager                                  Go to form "Drive
Version:                           <1.0.0.1052>            Management"
Status:                            <Enabled>

▶ Key Identifiers

Action(s) required!
Unencrypted drive(s) detected

▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management

                          F9=Reset to Defaults      F10=Save
↑↓=Move Highlight         <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2006-2021, Intel Corporation
```

After success revert in Drive Management, status changes to Unencrypted.

Figure 2-22. Drive Management - Unencrypted



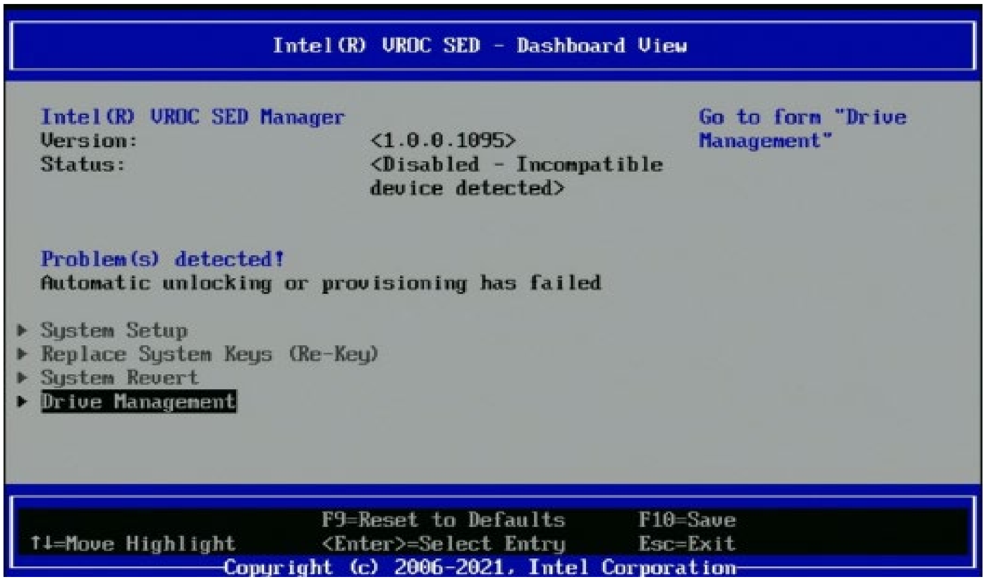
```
                 Intel(R) VROC SED - Drive Management

 Physical Drives with Self-Encrypting:              View the drive details
▶ INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB
   Port 4:1, Slot 10, CPU0, VMD0, BDF 81:00.0
   State: Unencrypted
▶ INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
   Port 4:5, Slot 11, CPU0, VMD0, BDF 82:00.0
   State: Locked
▶ INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
   Port 4:9, Slot 12, CPU0, VMD0, BDF 83:00.0
   State: Locked
▶ INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB
   Port 4:13, Slot 13, CPU0, VMD0, BDF 84:00.0
   State: Locked

 Physical Drives (Non-supported or without
                                                      ↓

 ↑↓=Move Highlight       <Enter>=Select Entry      Esc=Exit
            Copyright (c) 2006-2021, Intel Corporation
```

NOTE: After platform reboot drive is encrypted again because self-encrypting is enabled on the platform, to disable it on platform execute step 2.

2.5 Execute PSID Revert - Revert Drive to Factory Default

1. After system boot up, go to BIOS Menu, find Intel® VROC SED Manager then go to Drive Management.

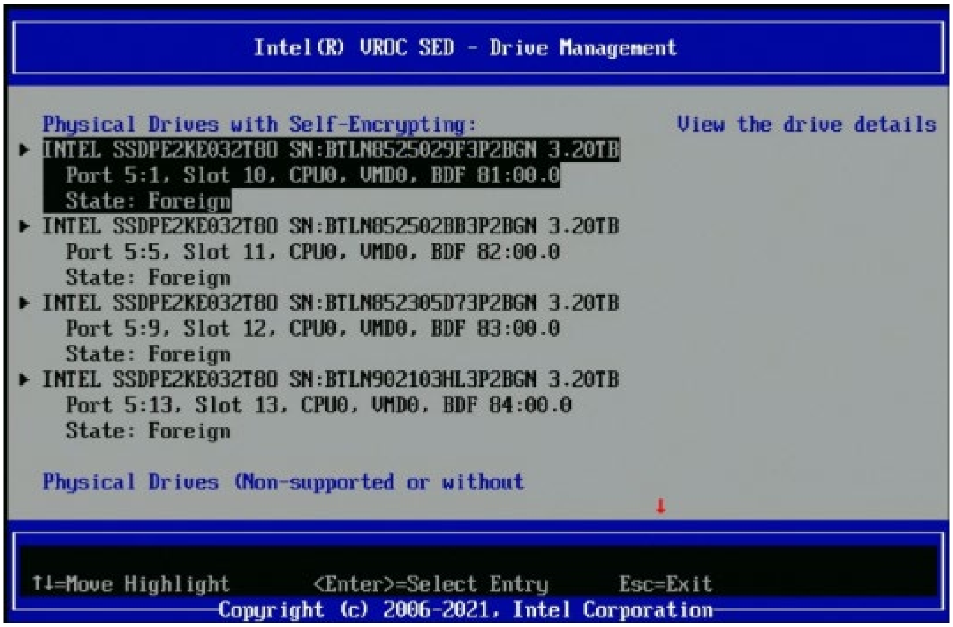
Figure 2-23. Dashboard View - Drive Management



```
                 Intel(R) VROC SED - Dashboard View

 Intel(R) VROC SED Manager                          Go to form "Drive
 Version:                <1.0.0.1095>               Management"
 Status:                 <Disabled - Incompatible
                         device detected>

 Problem(s) detected!
 Automatic unlocking or provisioning has failed

▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management

                         F9=Reset to Defaults     F10=Save
 ↑↓=Move Highlight       <Enter>=Select Entry     Esc=Exit
            Copyright (c) 2006-2021, Intel Corporation
```

2. Select the drive with status Foreign and click.

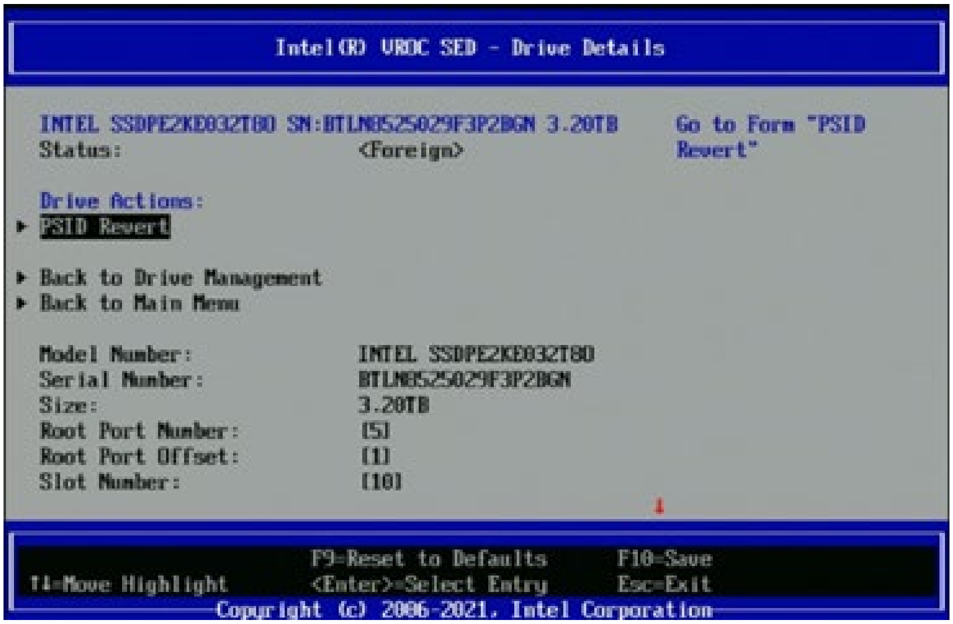
Figure 2-24. Dashboard View - Drive Management - Foreign



```
                 Intel(R) VROC SED - Drive Management

 Physical Drives with Self-Encrypting:               View the drive details
▶ INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB
   Port 5:1, Slot 10, CPU0, VMD0, BDF 81:00.0
   State: Foreign
▶ INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
   Port 5:5, Slot 11, CPU0, VMD0, BDF 82:00.0
   State: Foreign
▶ INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
   Port 5:9, Slot 12, CPU0, VMD0, BDF 83:00.0
   State: Foreign
▶ INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB
   Port 5:13, Slot 13, CPU0, VMD0, BDF 84:00.0
   State: Foreign

 Physical Drives (Non-supported or without
                                              ↓

 ↑↓=Move Highlight        <Enter>=Select Entry      Esc=Exit
            Copyright (c) 2006-2021, Intel Corporation
```

3. The following screen appears. Click PSID Revert.

Figure 2-25. Drive Details



```
                     Intel(R) VROC SED - Drive Details

  INTEL SSDPE2KE032T8O SN:BTLN8525029F3P2BGN 3.20TB      Go to Form "PSID
  Status:                      <Foreign>                 Revert"

  Drive Actions:
▶ PSID Revert

▶ Back to Drive Management
▶ Back to Main Menu

  Model Number:                INTEL SSDPE2KE032T8O
  Serial Number:               BTLN8525029F3P2BGN
  Size:                        3.20TB
  Root Port Number:            [5]
  Root Port Offset:            [1]
  Slot Number:                 [10]

                             F9=Reset to Defaults      F10=Save
 ↑↓=Move Highlight           <Enter>=Select Entry      Esc=Exit
                  Copyright (c) 2006-2021, Intel Corporation
```

4. Enter the 32-character PSID. This is printed on the drive case.

Figure 2-26. PSID

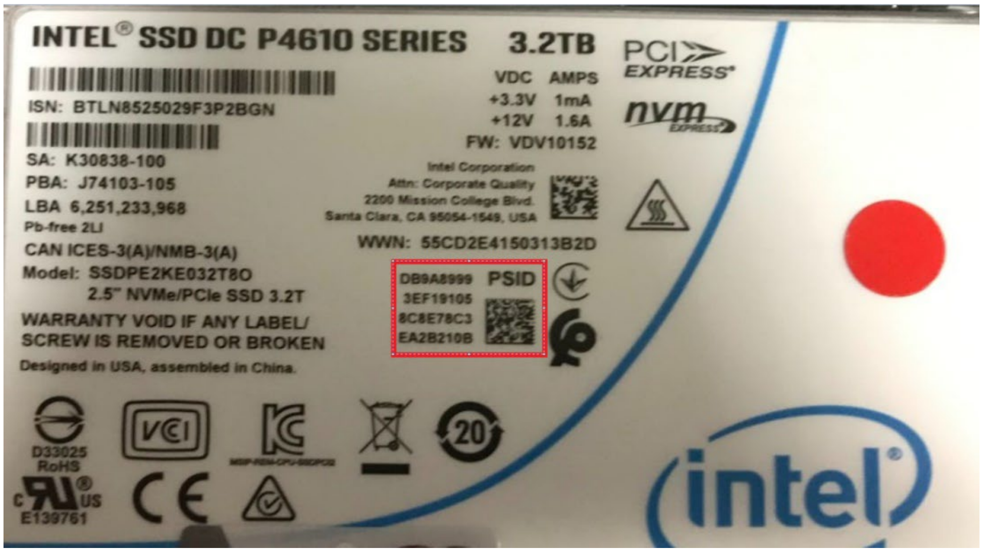
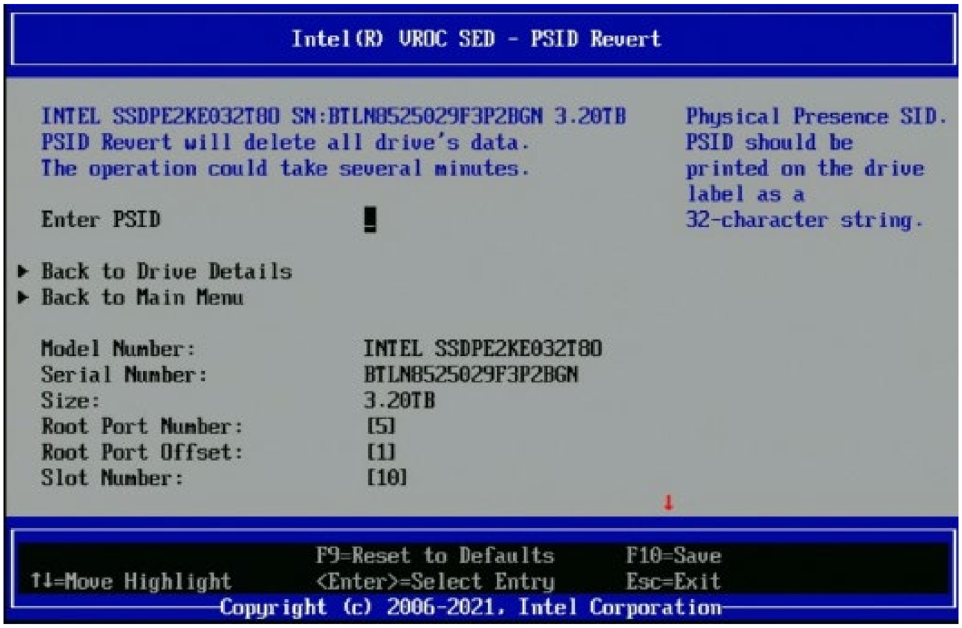


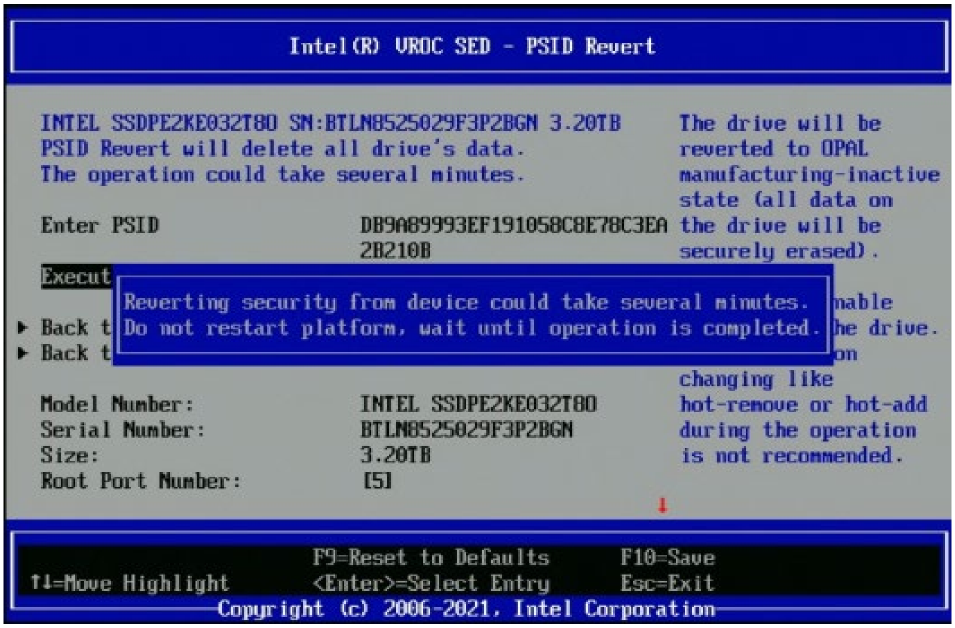
Figure 2-27. PSID Revert



```
                    Intel(R) VROC SED - PSID Revert

  INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB    Physical Presence SID.
  PSID Revert will delete all drive's data.            PSID should be
  The operation could take several minutes.            printed on the drive
                                                        label as a
  Enter PSID                                            32-character string.

▶ Back to Drive Details
▶ Back to Main Menu

  Model Number:              INTEL SSDPE2KE032T80
  Serial Number:             BTLN8525029F3P2BGN
  Size:                      3.20TB
  Root Port Number:          [5]
  Root Port Offset:          [1]
  Slot Number:               [10]

                           F9=Reset to Defaults       F10=Save
 ↑↓=Move Highlight         <Enter>=Select Entry       Esc=Exit
                 Copyright (c) 2006-2021, Intel Corporation
```

The following message appears.

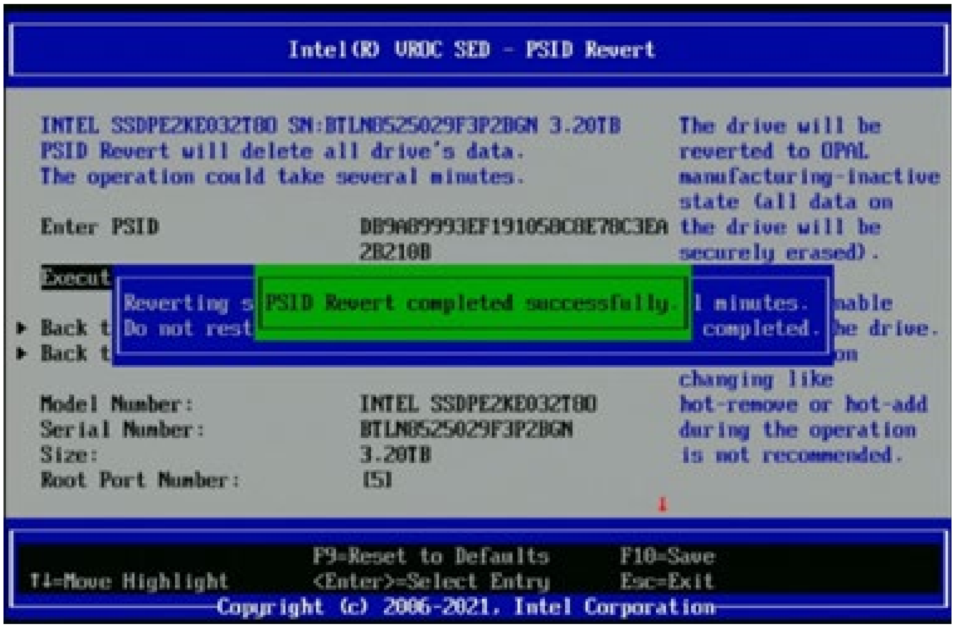
Figure 2-28. PSID Revert Massage



```
                    Intel(R) VROC SED - PSID Revert

  INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB    The drive will be
  PSID Revert will delete all drive's data.            reverted to OPAL
  The operation could take several minutes.            manufacturing-inactive
                                                        state (all data on
  Enter PSID                 DB9A89993EF191058C8E78C3EA the drive will be
                             2B210B                     securely erased).
  Execut
       Reverting security from device could take several minutes.  nable
▶ Back t Do not restart platform, wait until operation is completed. he drive.
▶ Back t                                                           on
                                                        changing like
  Model Number:              INTEL SSDPE2KE032T80      hot-remove or hot-add
  Serial Number:             BTLN8525029F3P2BGN        during the operation
  Size:                      3.20TB                     is not recommended.
  Root Port Number:          [5]

                           F9=Reset to Defaults       F10=Save
 ↑↓=Move Highlight         <Enter>=Select Entry       Esc=Exit
                 Copyright (c) 2006-2021, Intel Corporation
```

After successful revert, the following screen appears.

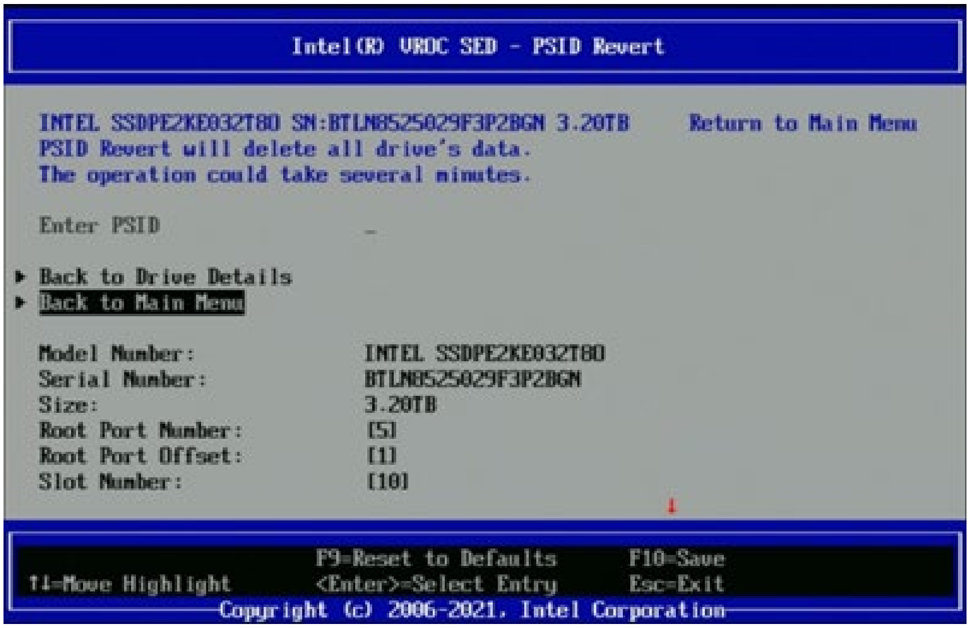
Figure 2-29. PSID Revert – Completed Successfully Massage



```
                         Intel(R) VROC SED - PSID Revert

INTEL SSDPE2KE032T8O SN:BTLN8525029F3P2BGN 3.20TB       The drive will be
PSID Revert will delete all drive's data.               reverted to OPAL
The operation could take several minutes.               manufacturing-inactive
                                                        state (all data on
Enter PSID                    DB9A89993EF191058C8E78C3EA the drive will be
                              2B210B                    securely erased).
Execut
        Reverting s PSID Revert completed successfully. l minutes.  nable
▶ Back t Do not rest                                    completed.  he drive.
▶ Back t                                                            on
                                                        changing like
Model Number:                 INTEL SSDPE2KE032T8O      hot-remove or hot-add
Serial Number:                BTLN8525029F3P2BGN        during the operation
Size:                         3.20TB                    is not recommended.
Root Port Number:             [5]

                              F9=Reset to Defaults      F10=Save
↑↓=Move Highlight             <Enter>=Select Entry      Esc=Exit
                  Copyright (c) 2006-2021, Intel Corporation
```

5. Return to Main Menu.

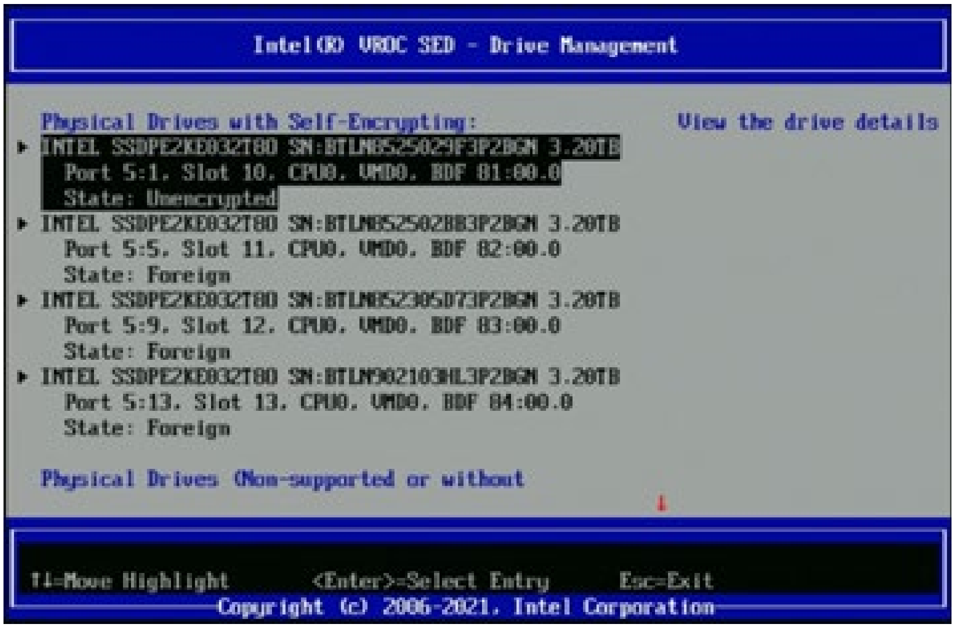
Figure 2-30. PSID Revert –Main Menu



```
                         Intel(R) VROC SED - PSID Revert

INTEL SSDPE2KE032T8O SN:BTLN8525029F3P2BGN 3.20TB       Return to Main Menu
PSID Revert will delete all drive's data.
The operation could take several minutes.

Enter PSID                     _

▶ Back to Drive Details
▶ Back to Main Menu

Model Number:                  INTEL SSDPE2KE032T8O
Serial Number:                 BTLN8525029F3P2BGN
Size:                          3.20TB
Root Port Number:              [5]
Root Port Offset:              [1]
Slot Number:                   [10]

                               F9=Reset to Defaults     F10=Save
↑↓=Move Highlight              <Enter>=Select Entry     Esc=Exit
                  Copyright (c) 2006-2021, Intel Corporation
```

6. Go to Drive Management. The status for the drive is Unencrypted.

Figure 2-31. Drive Management - Unencrypted



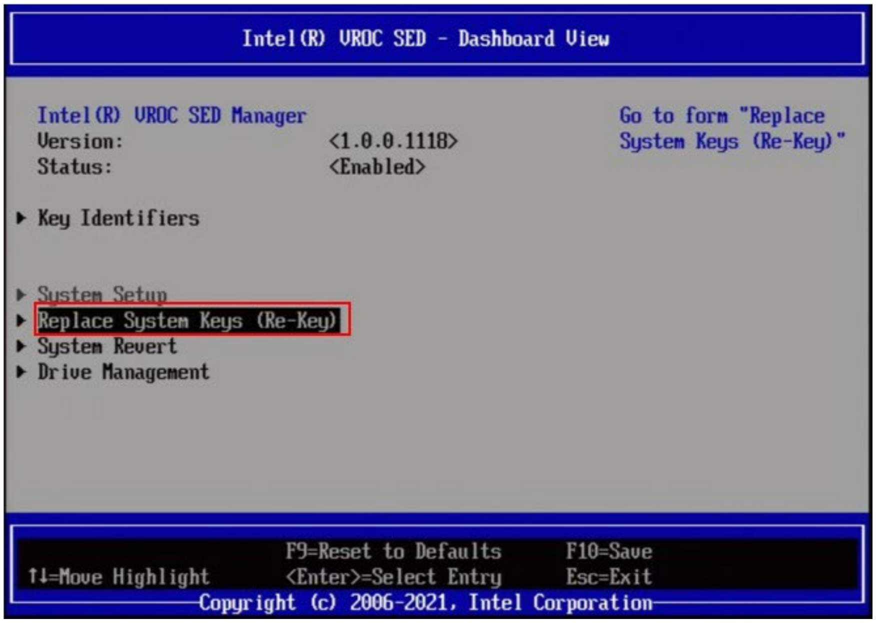
```
                    Intel(R) VROC SED - Drive Management

  Physical Drives with Self-Encrypting:                   View the drive details
▶ INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB
    Port 5:1. Slot 10. CPU0. VMD0. BDF 81:00.0
    State: Unencrypted
▶ INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB
    Port 5:5. Slot 11. CPU0. VMD0. BDF 82:00.0
    State: Foreign
▶ INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB
    Port 5:9. Slot 12. CPU0. VMD0. BDF 83:00.0
    State: Foreign
▶ INTEL SSDPE2KE032T80 SN:BTLM902103HL3P2BGN 3.20TB
    Port 5:13. Slot 13. CPU0. VMD0. BDF 84:00.0
    State: Foreign

  Physical Drives (Non-supported or without
                                                       ↓

 ↑↓=Move Highlight        <Enter>=Select Entry        Esc=Exit
              Copyright (c) 2006-2021. Intel Corporation
```

NOTE: After successful PSID revert, rebooting the platform is required.

2.6 Replace System Keys (Rekey) – Perform a Change of All Keys

1. After the system boots up, go to the BIOS menu, find Intel® VROC SED Manager then enter System Revert. All secured drives are displayed.

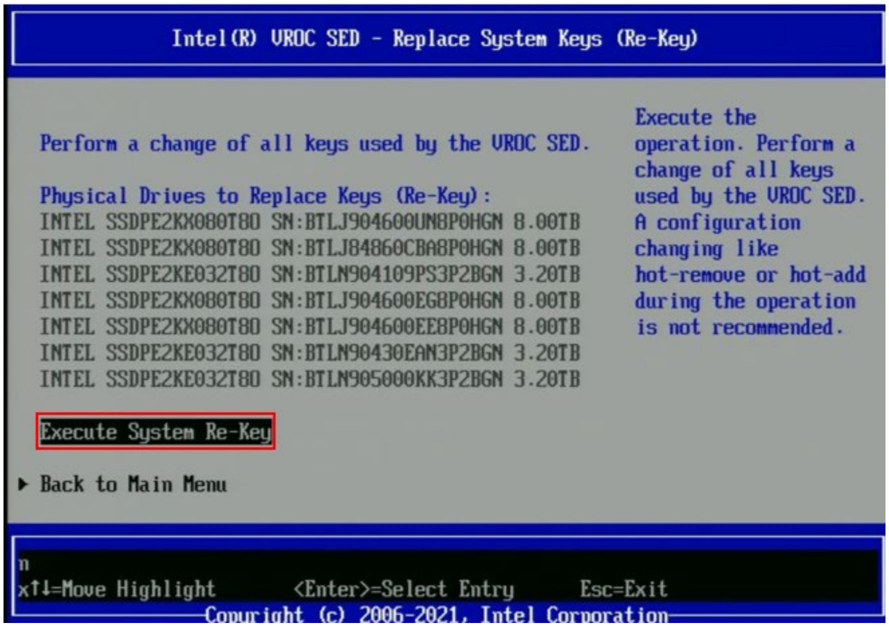
Figure 2-32. Dashboard View – Re-Key



```
                 Intel(R) VROC SED - Dashboard View

 Intel(R) VROC SED Manager                            Go to form "Replace
 Version:                 <1.0.0.1118>                System Keys (Re-Key)"
 Status:                  <Enabled>

▶ Key Identifiers

▶ System Setup
▶ Replace System Keys (Re-Key)
▶ System Revert
▶ Drive Management

                         F9=Reset to Defaults      F10=Save
 ↑↓=Move Highlight       <Enter>=Select Entry      Esc=Exit
               Copyright (c) 2006-2021, Intel Corporation
```

2. Select Execute System Re-Key.

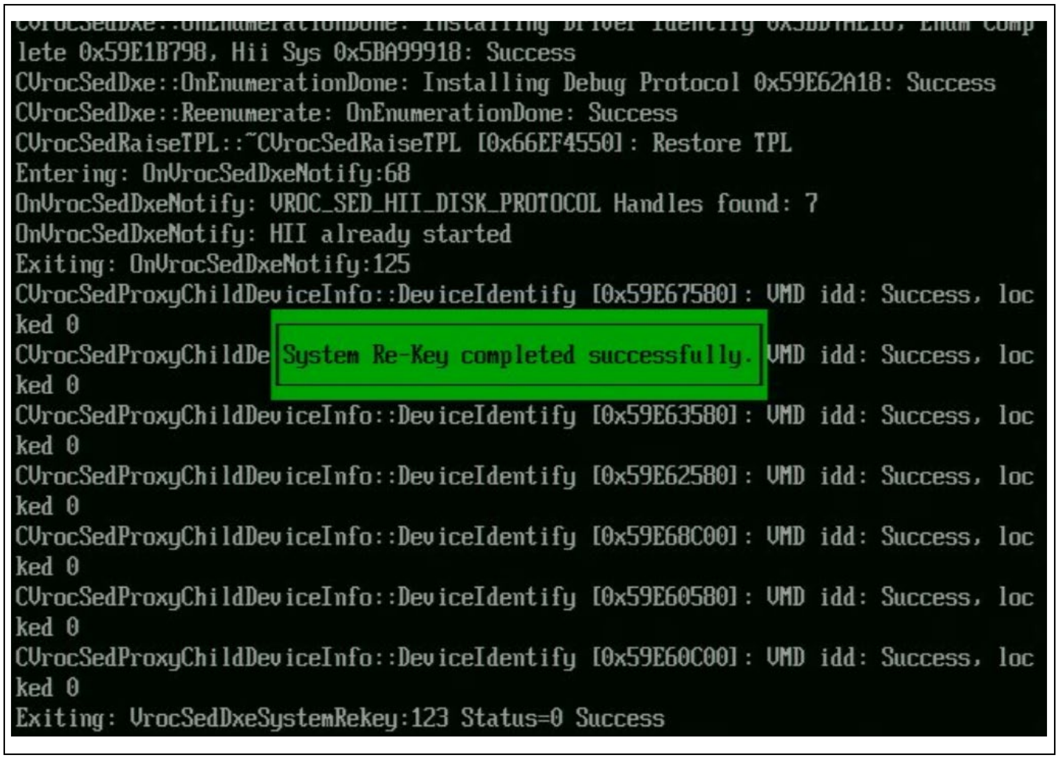
Figure 2-33. Replace System Keys (Re-Key)



```
          Intel(R) VROC SED - Replace System Keys (Re-Key)

                                                          Execute the
 Perform a change of all keys used by the VROC SED.      operation. Perform a
                                                          change of all keys
 Physical Drives to Replace Keys (Re-Key):                used by the VROC SED.
 INTEL SSDPE2KX080T80 SN:BTLJ904600UN8P0HGN 8.00TB        A configuration
 INTEL SSDPE2KX080T80 SN:BTLJ84860CBA8P0HGN 8.00TB        changing like
 INTEL SSDPE2KE032T80 SN:BTLN904109PS3P2BGN 3.20TB        hot-remove or hot-add
 INTEL SSDPE2KX080T80 SN:BTLJ904600EG8P0HGN 8.00TB        during the operation
 INTEL SSDPE2KX080T80 SN:BTLJ904600EE8P0HGN 8.00TB        is not recommended.
 INTEL SSDPE2KE032T80 SN:BTLN90430EAN3P2BGN 3.20TB
 INTEL SSDPE2KE032T80 SN:BTLN905000KK3P2BGN 3.20TB

 Execute System Re-Key

▶ Back to Main Menu

n
x↑↓=Move Highlight       <Enter>=Select Entry       Esc=Exit
               Copyright (c) 2006-2021, Intel Corporation
```

The following screen appears.

Figure 2-34. Re-Key Completed Successfully Message

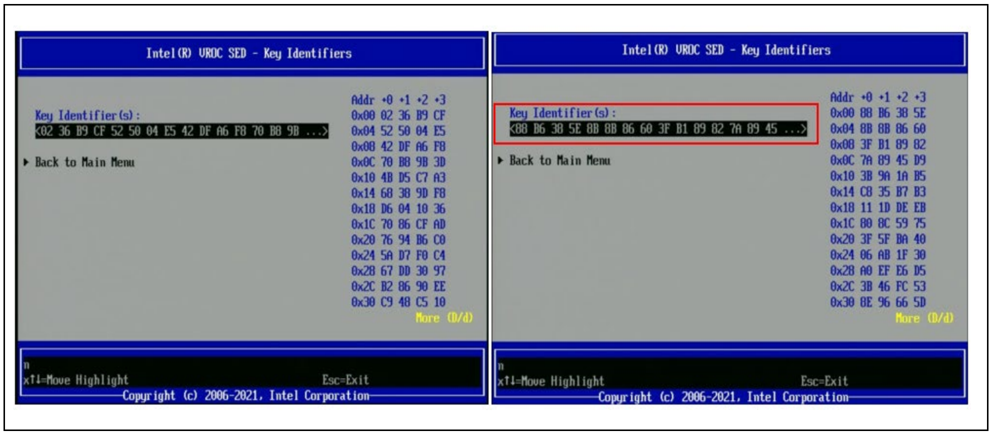


```
CVrocSedDxe::OnEnumerationDone: Installing Driver Identify 0x5DD1AE18, Enum Comp
lete 0x59E1B798, Hii Sys 0x5BA99918: Success
CVrocSedDxe::OnEnumerationDone: Installing Debug Protocol 0x59E62A18: Success
CVrocSedDxe::Reenumerate: OnEnumerationDone: Success
CVrocSedRaiseTPL::~CVrocSedRaiseTPL [0x66EF4550]: Restore TPL
Entering: OnVrocSedDxeNotify:68
OnVrocSedDxeNotify: VROC_SED_HII_DISK_PROTOCOL Handles found: 7
OnVrocSedDxeNotify: HII already started
Exiting: OnVrocSedDxeNotify:125
CVrocSedProxyChildDeviceInfo::DeviceIdentify [0x59E67580]: VMD idd: Success, loc
ked 0
CVrocSedProxyChildDe System Re-Key completed successfully. VMD idd: Success, loc
ked 0
CVrocSedProxyChildDeviceInfo::DeviceIdentify [0x59E63580]: VMD idd: Success, loc
ked 0
CVrocSedProxyChildDeviceInfo::DeviceIdentify [0x59E62580]: VMD idd: Success, loc
ked 0
CVrocSedProxyChildDeviceInfo::DeviceIdentify [0x59E68C00]: VMD idd: Success, loc
ked 0
CVrocSedProxyChildDeviceInfo::DeviceIdentify [0x59E60580]: VMD idd: Success, loc
ked 0
CVrocSedProxyChildDeviceInfo::DeviceIdentify [0x59E60C00]: VMD idd: Success, loc
ked 0
Exiting: VrocSedDxeSystemRekey:123 Status=0 Success
```

3. Return to the SED Manager Main Menu and select Key Identifier.

The following screen appears.

Figure 2-35. Key Identifiers



```
Intel(R) VROC SED - Key Identifiers

Key Identifier(s):                                     Addr +0 +1 +2 +3
<02 36 B9 CF 52 50 04 E5 42 DF A6 F8 70 B8 9B ...>     0x00 02 36 B9 CF
                                                       0x04 52 50 04 E5
▶ Back to Main Menu                                    0x08 42 DF A6 F8
                                                       0x0C 70 B8 9B 3D
                                                       0x10 4B D5 C7 A3
                                                       0x14 68 38 9D F8
                                                       0x18 D6 04 10 36
                                                       0x1C 70 86 CF AD
                                                       0x20 76 94 B6 C0
                                                       0x24 5A D7 F0 C4
                                                       0x28 67 DD 30 97
                                                       0x2C B2 86 90 EE
                                                       0x30 C9 48 C5 10
                                                             More (D/d)
n
x↑↓=Move Highlight                              Esc=Exit
Copyright (c) 2006-2021, Intel Corporation
```

```
Intel(R) VROC SED - Key Identifiers

Key Identifier(s):                                     Addr +0 +1 +2 +3
<88 B6 38 5E 8B 8B 86 60 3F B1 89 82 7A 89 45 ...>     0x00 88 B6 38 5E
                                                       0x04 8B 8B 86 60
▶ Back to Main Menu                                    0x08 3F B1 89 82
                                                       0x0C 7A 89 45 D9
                                                       0x10 3B 9A 1A B5
                                                       0x14 C8 35 B7 B3
                                                       0x18 11 1D DE EB
                                                       0x1C 80 8C 59 75
                                                       0x20 3F 5F BA 40
                                                       0x24 06 AB 1F 30
                                                       0x28 A0 EF E6 D5
                                                       0x2C 3B 46 FC 53
                                                       0x30 8E 96 66 5D
                                                             More (D/d)
n
x↑↓=Move Highlight                              Esc=Exit
Copyright (c) 2006-2021, Intel Corporation
```

NOTE: During Re-Key operation, the configuration change like Hot-remove or Hot-add is not recommended.

§§

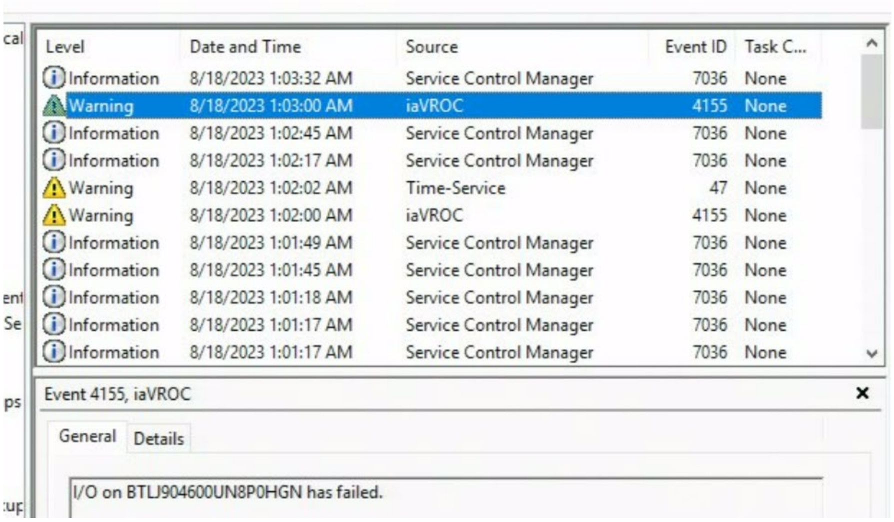
3 Limitations

When the disk has been SED Encrypted by VROC UEFI, A configuration changing like hot-remove or hot-add during the operation under OS level is not recommended so far till later VROC support SED configuration changing from OS level.

3.1 Windows*

SED hot-plug is not recommended on Windows when a drive has been VROC encrypted, the hot-plug disk will no longer be able to access correctly as below and will have the Volume rebuild will not trigger. The system reboot is required to have VROC UEFI driver to over-provision to unlock the encrypted disk to be able to access again.

Figure 3-1. Windows* Warning



Level	Date and Time	Source	Event ID	Task C...
Information	8/18/2023 1:03:32 AM	Service Control Manager	7036	None
Warning	8/18/2023 1:03:00 AM	iaVROC	4155	None
Information	8/18/2023 1:02:45 AM	Service Control Manager	7036	None
Information	8/18/2023 1:02:17 AM	Service Control Manager	7036	None
Warning	8/18/2023 1:02:02 AM	Time-Service	47	None
Warning	8/18/2023 1:02:00 AM	iaVROC	4155	None
Information	8/18/2023 1:01:49 AM	Service Control Manager	7036	None
Information	8/18/2023 1:01:45 AM	Service Control Manager	7036	None
Information	8/18/2023 1:01:18 AM	Service Control Manager	7036	None
Information	8/18/2023 1:01:17 AM	Service Control Manager	7036	None
Information	8/18/2023 1:01:17 AM	Service Control Manager	7036	None

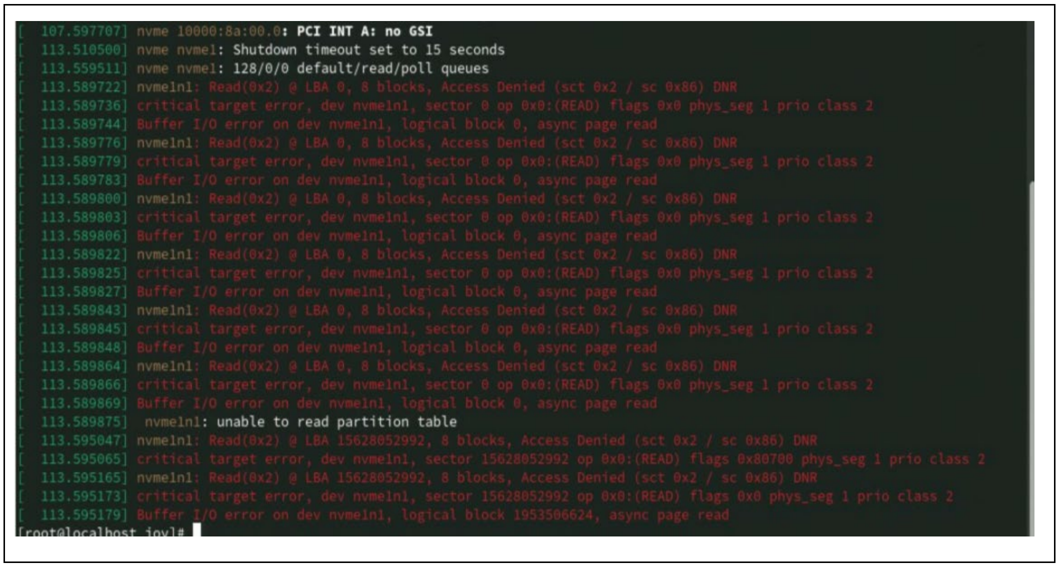
Event 4155, iaVROC

I/O on BTLJ904600UN8P0HGN has failed.

3.2 Linux*

SED hot-plug is not recommended on Linux* when a drive has been VROC encrypted, the hot-plug disk will no longer be able to read correctly as below, and the volume rebuild will not be triggered. The system reboot is required to have VROC UEFI driver to over-provision to unlock the encrypted disk to be able to access again.

Figure 3-2. Linux* Warning



```
[  107.597707] nvme 10000:8a:00.0: PCI INT A: no GSI
[  113.510500] nvme nvme1: Shutdown timeout set to 15 seconds
[  113.559511] nvme nvme1: 128/0/0 default/read/poll queues
[  113.589722] nvme1n1: Read(0x2) @ LBA 0, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.589736] critical target error, dev nvme1n1, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2
[  113.589744] Buffer I/O error on dev nvme1n1, logical block 0, async page read
[  113.589776] nvme1n1: Read(0x2) @ LBA 0, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.589779] critical target error, dev nvme1n1, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2
[  113.589783] Buffer I/O error on dev nvme1n1, logical block 0, async page read
[  113.589800] nvme1n1: Read(0x2) @ LBA 0, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.589803] critical target error, dev nvme1n1, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2
[  113.589806] Buffer I/O error on dev nvme1n1, logical block 0, async page read
[  113.589822] nvme1n1: Read(0x2) @ LBA 0, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.589825] critical target error, dev nvme1n1, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2
[  113.589827] Buffer I/O error on dev nvme1n1, logical block 0, async page read
[  113.589843] nvme1n1: Read(0x2) @ LBA 0, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.589845] critical target error, dev nvme1n1, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2
[  113.589848] Buffer I/O error on dev nvme1n1, logical block 0, async page read
[  113.589864] nvme1n1: Read(0x2) @ LBA 0, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.589866] critical target error, dev nvme1n1, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2
[  113.589869] Buffer I/O error on dev nvme1n1, logical block 0, async page read
[  113.589875]  nvme1n1: unable to read partition table
[  113.595047] nvme1n1: Read(0x2) @ LBA 15628052992, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.595065] critical target error, dev nvme1n1, sector 15628052992 op 0x0:(READ) flags 0x80700 phys_seg 1 prio class 2
[  113.595165] nvme1n1: Read(0x2) @ LBA 15628052992, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR
[  113.595173] critical target error, dev nvme1n1, sector 15628052992 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2
[  113.595179] Buffer I/O error on dev nvme1n1, logical block 1953506624, async page read
[root@localhost iov]#
```

§§