

## Intel<sup>®</sup> Virtual RAID on CPU (Intel<sup>®</sup> VROC) Self-Encrypting Drive Feature

**User Guide** 

**Revision 1.1** 

March 2024

Document Number:759299

# intel

This document contains information on products in the design phase of development. The information here is subject to change without notice. Do not finalize a design with this information.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis. You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

All product plans and roadmaps are subject to change without notice.

The products described may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Altering clock frequency, voltage, or memory interface speeds may void any product warranties and reduce stability, security, performance, and life of the processor and other components. Intel has not validated processor running memory above Plan-Of-Record (POR) speed. DRAM/DIMM devices should support desired speed, check with DRAM/DIMM vendors for details. System manufacturers are responsible for all validation and assume the risk of any stability, security, performance, or other functional issues resulting from such alterations.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries.

\*Other names and brands may be claimed as the property of others.

Copyright© 2023-2024 Intel Corporation. All rights reserved.

# intel

## Contents

1	Introd	duction	6
	1.1	SED and OPAL Overview	6
2	Intel®	<sup>9</sup> VROC SED Functions	7
	2.1	How to Enable Intel <sup>®</sup> VROC SED in BIOS	7
	2.2	Enable Self-Encrypting	7
	2.3	System Revert	10
	2.4	Drive Revert	14
	2.5	Execute PSID Revert - Revert Drive to Factory Default	18
	2.6	Replace System Keys (Rekey) – Perform a Change of All Keys	23
3	Limita	ations	26
	3.1	Windows*	
	3.2	Linux*	

## **Figures**

Figure 2-1. EDKII Menu	7
Figure 2-2. Dashboard View	8
Figure 2-3. System Setup	8
Figure 2-4. System Completed Screen	9
Figure 2-4. Dashboard View - Enabled	9
Figure 2-6. Drive Management	10
Figure 2-7. Dashboard View – System Revert	10
Figure 2-8. Dashboard View – System Revert Confirm Box	11
Figure 2-8. System Revert	11
Figure 2-10. System Revert – Completed Message	12
Figure 2-11. System Revert – Successfully Completed Message	12
Figure 2-12. Dashboard View - Disabled	13
Figure 2-13. Drive Management – Not Provisioned	13
Figure 2-14. Dashboard View - Drive Management	14
Figure 2-15. Drive Management	14
Figure 2-16. Drive Details	15
Figure 2-17. Secure Erase Drive for Removal – Confirm Box	15
Figure 2-18. Secure Erase Drive for Removal	16
Figure 2-19. Secure Erase Drive for Removal- Completed Successfully Message	16
Figure 2-20. Secure Erase Drive for Removal– Back to Main Menu	17
Figure 2-21. Dashboard View – Drive Management	17
Figure 2-22. Drive Management - Unencrypted	18
Figure 2-14. Dashboard View - Drive Management	19
Figure 2-24. Dashboard View - Drive Management - Foreign	19
Figure 2-25. Drive Details	20
Figure 2-26. PSID	20
Figure 2-26. PSID Revert	21
Figure 2-28. PSID Revert Massage	21
Figure 2-29. PSID Revert – Completed Successfully Massage	22
Figure 2-30. PSID Revert – Main Menu	22
Figure 2-31. Drive Management - Unencrypted	23
Figure 2-32. Dashboard View – Re-Key	24
Figure 2-33. Replace System Keys (Re-Key)	24



Figure 2-34. Re-Key Completed Successfully Message	. 25
Figure 2-35. Key Identifiers	. 25
Figure 3-1. Windows* Warning	. 26
Figure 3-2. Linux* Warning	. 27



## **Revision History**

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

§§



# **1** Introduction

This document describes the operations of the Intel<sup>®</sup> Virtual RAID on CPU (Intel<sup>®</sup> VROC) Self-Encrypting Drive feature for the Intel<sup>®</sup> Virtual RAID on CPU (Intel<sup>®</sup> VROC) products based on Intel<sup>®</sup> Xeon<sup>®</sup> 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.
- 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".

§§

# intel.

# 2 Intel<sup>®</sup> VROC SED Functions

#### **Configuration:**

- 1. HW: Intel® Whitley CRB
- 2. BIOS: Whitley\_ICX BKC BIOS
- 3. Intel<sup>®</sup> 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<sup>®</sup> VROC SED in BIOS

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

#### Figure 2-1. EDKII Menu

All Cpu Information	Help for Intel(R)
Platform Driver Override selection	UROC SED Manager
Ils 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	
	1

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

### 2.2 Enable Self-Encrypting

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

#### Figure 2-2. Dashboard View

Intel(R) UROC SE	D Manager	Go to form "System
Status:	<disabled></disabled>	Secup
Sucton Sotun		
oystem betup		
Replace System K	eys (Re-Key)	
Replace System Ke System Revert	eys (Re-Key)	
Replace System Ke System Revert Drive Management	eys (Re-Key)	
Replace System Ka System Revert Drive Management	eys (Re-Key)	
Replace System Ka System Revert Drive Management	eys (Re-Key)	
Replace System Ka System Revert Drive Management	eys (Re-Key)	
Replace System Ko System Revert Drive Management	eys (Re-Key)	
- Replace System Ko - System Revert - Drive Management	eys (Re-Key) F9=Reset to Defaults	F10=Save

**NOTE:** If no NVMe driver is present in system, Intel<sup>®</sup> VROC SED manager and Intel<sup>®</sup> 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:

	Generates the System
Enable security on the system.	Key and prepares the
	system for secured
Physical Drives to provision:	KHID arrays and
THIEF SODESKEDSSIDD ON BEINDESSOEDSSDON 3 SOLD	drives. It also
INITEL SOUPLEARED STOR ON DILLNGS2305073P2B6N 3.2018	enables encryption on
INITE CODDECKEDSTRO ON DEINOCSCOSDESDERN 3.501B	all the nume drives
INIET 22065546035190 20:BITU0252053L365860 3:5018	In the system.
Everyte System Setur	H configuration
Execute System Setup	bot-romous or bot-add
Back to Main Monu	during the operation
back to harn hend	is not recommended
	15 Hot recommended.

Figure 2-3. System Setup

When successful, the following screen appears.



Figure 2-4. System Completed Screen

Enable security on the system.	Generates the System Key and prepares the
Munical Driver to provision.	system for secured
TNTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TE	drives. It also
INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TE	enables encryption of
IN Setup Security configuration on the system co Execute System Setup	mpleted successfully. changing like hot-remove or hot-ad
Back to Main Menu	during the operation is not recommended.

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

Figure 2-5. Dashboard View - Enabled



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

# intel



Intel(R) UROC SED - Drive Managem	ent
<ul> <li>Physical Drives with Self-Encrypting:</li> <li>INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TE Port 4:1, Slot 10, CPU0, VMD0, BDF 81:00.0</li> <li>State: Unlocked</li> <li>INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB Port 4:5, Slot 11, CPU0, VMD0, BDF 82:00.0 State: Unlocked</li> <li>INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB Port 4:9, Slot 12, CPU0, VMD0, BDF 83:00.0 State: Unlocked</li> <li>INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB Port 4:13, Slot 13, CPU0, VMD0, BDF 84:00.0 State: Unlocked</li> </ul>	View the drive details
Physical Drives (Non-supported or without	1
↑↓=Move Highlight <enter>=Select Entry Es Copyright (c) 2006-2021, Intel Corpo</enter>	c=Exit ration

### **2.3** System Revert

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





2. Check the Confirm Box.





Physical Drives t INTEL SSDPE2KE032 INTEL SSDPE2KE032	o Revert: TRO SN-RTI NGO2103HI 3D		
INTEL SSDPE2KE032 INTEL SSDPE2KE032 INTEL SSDPE2KE032	T80 SN:BTLN852305D73P T80 SN:BTLN852502BB3P T80 SN:BTLN852502BB3P T80 SN:BTLN8525029F3P	2BGN 3.20TB 2BGN 3.20TB 2BGN 3.20TB 2BGN 3.20TB	
All secured drive Reverting securit several minutes Confirm	s will be reverted am y from all drives cou	d data erased ld take	
Back to Main Menu			

3. Execute System Revert

#### Figure 2-9. System Revert

Int	el(R) VROC SED - Syste	m Revert
Revert security configu	ration from the system	
Dhucical Drives to Pour		
INTEL SSDPE2KE032T80 SM	:BTLN902103HL3P2BGN 3.	20TB
INTEL SSDPE2KE032T80 SM	:BTLN852305D73P2BGN 3.	20TB
INTEL SSDPE2KE032T80 SM	BTLN852502BB3P2BGN 3.	20TB
INTEL SSDPEZKE032T80 SP	BTLN8525029F3P2BGN 3.	2018
All secured drives will	be reverted and data	erased.
Reverting security from	all drives could take	
Several minutes.	TY1	
Execute Sustem Revert		
		1
	F9=Reset to Defaults	F10=Save
†↓=Move Highlight	<spacebar>Toggle Check</spacebar>	box Esc=Exit
	t (c) 2006-2021, Intel	Corporation

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

# intel.



	Destroys the System
Revert security configuration from the system.	Key.
Phusical Drives to Revert:	will be reverted to
INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB	OPAL manufacturing
INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB	inactive state (eras
INTEL Reverting security from devices could take so Do not restart platform, wait until operation	everal minutes. on n is completed. hot-ad
INTEL Reverting security from devices could take so Do not restart platform, wait until operation All se Reverting security from all drives could take	everal minutes. n is completed. hot-ad during the operation
INTEL Reverting security from devices could take severing security from all drives could take several minutes.	everal minutes. on n is completed. hot-ad during the operation is not recommended.
INTEL Reverting security from devices could take set Do not restart platform, wait until operation All se Reverting security from all drives could take several minutes. Confirm [X] Frequeta Sustan Revert	everal minutes. on n is completed. hot-ad during the operation is not recommended.
INTEL Reverting security from devices could take so Do not restart platform, wait until operation All se Reverting security from all drives could take several minutes. Confirm [X] Execute System Revert	everal minutes. n is completed. hot-ad during the operation is not recommended.
INTEL Reverting security from devices could take security from all drives could take several minutes. Confirm [X] Execute System Revert	everal minutes. n is completed. during the operation is not recommended.
INTEL Reverting security from devices could take so Do not restart platform, wait until operation All se Reverting security from all drives could take several minutes. Confirm [X] Execute System Revert F9=Reset to Defaults F10	everal minutes. n is completed. during the operation is not recommended.

5. After successful Revert, the following screen appears.

#### Figure 2-11. System Revert – Successfully Completed Message

Revert security conf	iguration from the sustem	Destroys the System
Never e Sceur reg com	iguration from the system.	All secured drives
Physical Drives to R	evert:	will be reverted to
INTEL SSDPE2KE032T80	SN:BTLN902103HL3P2BGN 3.20TB	OPAL manufacturing
INTEL SSDPE2KE032T80	SN:BTLN852305D73P2BGN 3.20TB	inactive state (eras
All se Reverting security f	rom all drives could take	during the operation
several minutes.		is not recommended.
several minutes. Confirm	נאז	is not recommended.
several minutes. Confirm Execute System Rever	CX3	is not recommended.

The Dashboard View changes to Disabled.



Figure 2-12. Dashboard View - Disabled

Intel(R) UROC SED - Dashboard View		
Intel(R) VROC SED Manager Version: <1.0.0.10 Status: <disabled< td=""><td>52&gt; &gt;</td></disabled<>	52> >	
<ul> <li>System Setup</li> <li>Replace System Keys (Re-Key)</li> <li>System Revert</li> <li>Drive Management</li> </ul>		
F9=Reset to D	efaults F10=Save	
↑↓=Move Highlight <enter>=Selec Copyright (c) 2006-20</enter>	t Entry Esc=Exit 21, Intel Corporation	

In Drive Management, the state drive is Not Provisioned.

Figure 2-13. Drive Management – Not Provisioned

Physical Drives with Self-Encrypting: INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB Port 4.1 Slot 10 CPU0, VMD0, BDF 81:00.0	View the drive details
<ul> <li>State: Unencrypted</li> <li>INIEL SSDFEZKE03Z180 SN:BTLN852305D73P2BGN 3.20TB Port 4:5, Slot 11, CPU0, VMD0, BDF 82:00.0 State: Unencrypted</li> <li>INTEL SSDFEZKE03ZT80 SN:BTLN852502BB3P2BGN 3.20TB Port 4:9, Slot 12, CPU0, VMD0, BDF 83:00.0 State: Unencrypted</li> </ul>	
<ul> <li>INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TB Port 4:13, Slot 13, CPU0, VMD0, BDF 84:00.0 State: Unencrypted</li> </ul>	
Physical Drives (Non-supported or without	4



## 2.4 Drive Revert

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



Intel(R) UROC SE	D Manager	
Version:	<1.0.0.1052>	
Status:	<enabled></enabled>	
Key Identifiers		
System Setup Replace System K Sustem Revert	eys (Re-Key)	
Drive Management	J. States and the second second	

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

#### Figure 2-15. Drive Management





3. Click Prepare drive for removal (Secure Erase)

#### Figure 2-16. Drive Details

Intel(R) UROC SED - Drive Details		
INTEL SSDPE2KE032T80 Status: Drive Actions:	SN:BTLN902103HL3P2BGN 3.20TB <unlocked></unlocked>	Go to Form "Secure Erase Drive for Removal"
Back to Drive Manage Back to Main Menu	ment	
Model Number:	INTEL SSDPE2KE032T80	
Model Number: Serial Number: Size: Poot Poort Number:	INTEL SSDPE2KE032T80 BTLN902103HL3P2BGN 3.20TB	

4. Check the Confirm Box.

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

1 201:01103021030L3P2060 3.2010	
vill delete Key and Irive's data will be erased. take several minutes	
s	
INTEL SSDPE2KE032T80 BTLN902103HL3P2BGN	
2 2070	
	vill delete Key and Irive's data will be erased. take several minutes IS INTEL SSDPE2KE032T80 BTLN902103HL3P2BGN

5. Execute Secure Erase - Prepare drive for removal.

Figure 2-18. Secure Erase Drive for Removal

Intel(R) UR(	DC SED – Secure Erase Drive	for Removal
INTEL SSDPE2KE032T80 SM	N:BTLN902103HL3P2BGN 3.20TB	The drive will be reverted to OPAL
Security Reverting will	l delete Key and	manufacturing-inactiv
configuration. All drive's data will be erased.		state (all data on
The operation could take several minutes		the drive will be
Confirm	ראז	A configuration
Execute Secure Erase Dr	iue for Removal	changing like
		hot-remove or hot-add
▶ Back to Drive Details		during the operation
<ul> <li>Back to Main Menu</li> </ul>		is not recommended.
Madal Number	TNTEL CONFORTON	
Sorial Number:	THILL SSUPLEMEDSLIDU	
Size.	3 20TB	
5126.	5.2015	1
	F9=Reset to Defaults I	F10=Save
†↓=Move Highlight	<enter>=Select Entry I</enter>	Esc=Exit
Copyr igł	nt (c) 2006-2021, Intel Corp	poration

After a successful erase, the following screen appears.

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





6. Return to the Main Menu.

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

Intel(R)	JROC SED - Secure Erase Drive f	for Removal
INTEL SSDPE2KE032T80 Security Reverting w configuration. All du The operation could t	SN:BTLN902103HL3P2BGN 3.20TB ill delete Key and rive's data will be erased. take several minutes	Go back to "Drive Details" form of this drive
Confirm	[]	
Back to Main Menu Model Number: Serial Number: Size: Boot Port Number:	INTEL SSDPE2KE032T80 BTLN902103HL3P2BGN 3.20TB [4]	
t4=Move Highlight	F9=Reset to Defaults F1 <enter>=Select Entry Es</enter>	↓ 10=Save sc=Exit

7. Select Drive Management.

#### Figure 2-21. Dashboard View – Drive Management





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

Figure 2-22. Drive Management - Unencrypted



**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<sup>®</sup> VROC SED Manager then go to Drive Management.





THEET WY VALUE JED Hana	<b>Jer</b>	Go to form "Drive
Version: Status:	<1.0.0.1095> <disabled -="" incompatible<br="">device detected&gt;</disabled>	Management"
Problem(s) detected! Automatic unlocking or System Setup Replace System Keys (R System Revert	provisioning has failed e-Key)	

2. Select the drive with status Foreign and click.

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

<ul> <li>Physical Drives with Self-Encrypting:</li> <li>INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BGN 3.20TE Port 5:1, Slot 10, CPU0, UMD0, BDF 81:00.0 State: Foreign</li> <li>INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB Port 5:5, Slot 11, CPU0, UMD0, BDF 82:00.0 State: Foreign</li> <li>INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB Port 5:9, Slot 12, CPU0, UMD0, BDF 83:00.0 State: Foreign</li> <li>INTEL SSDPE2KE032T80 SN:BTLN902103HL3P2BGN 3.20TB Port 5:13, Slot 13, CPU0, UMD0, BDF 84:60.0 State: Foreign</li> </ul>	View the drive details
Physical Drives (Non-supported or without	

#### 3. The following screen appears. Click PSID Revert.

#### Figure 2-25. Drive Details

INTEL SSDPE2KE032T0	) SN:BTLNB525029F3P2BGN 3.20TE	Go to Form "PSID
status:	Croreigno	hever t
rive Actions:		
SID Revert		
lack to Drive Manage	ement	
lack to Main Menu		
Indal Number:	INTEL SSRPENED20100	
Secial Number:	RTI NSS25A29F3P2RCN	
Size:	3.2018	
Root Port Number:	[5]	
Root Port Offset:	ω.	
Slot Number:	[10]	
		4
	F9=Reset to Defaults	F10=Saue

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

#### Figure 2-26. PSID

INTEL® SSD DC P4610	SERIES 3.2TB VDC AMPS 43.3V 1mA 412V 1.6A FW: VDV10152 Intel Corporation Attr: Corporate Quality 2200 Massion College Bivd. Massion College Bivd. Attr: Corporate Quality 2000 Massion College Bivd. Massion College Bivd. M	PCIDE EXPRESS DUCE
	X @	(intel)



#### Figure 2-27. PSID Revert

INTEL SSDPE2KE032T80 PSID Revert will delu	SN:BTLN8525029F3P2BGN 3.20TB	Physical Presence SID PSID should be		
The operation could take several minutes.		printed on the drive		
Enter PSID		label as a 32-character string.		
Rack 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]			
		1		

The following message appears.

Figure 2-28. PSID Revert Massage



After successful revert, the following screen appears.

# intel.





5. Return to Main Menu.

#### Figure 2-30. PSID Revert - Main Menu

INTEL SSDPE2KE032T80 PSID Revert will dele The operation could t	SN:BTLN8525029F3P2BGN 3.20TB te all drive's data. ake several minutes.	Return to Main Menu
Enter PSID	-	
Rack to Drive Details		
Back to Main Menu		
Model Number:	INTEL SSDPE2KE032T80	
Serial Number:	BTLN8525029F3P2BGN	
Size:	3.20TB	
Root Port Number:	(5)	
Root Port Offset:	m	
Slot Number:	[10]	12
		1

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





Physical Drives with Self-Encrypting: INTEL SSDPE2KE032T80 SN:BTLN8525029F3P2BEN 3.20TE Port 5:1. Slot 10. CPU0. UMD0. BDF 81:00.0 State: Unencrypted INTEL SSDPE2KE032T80 SN:BTLN852502BB3P2BGN 3.20TB Port 5:5. Slot 11. CPU0. UMD0. BDF 82:00.0 State: Foreign INTEL SSDPE2KE032T80 SN:BTLN852305D73P2BGN 3.20TB Port 5:9. Slot 12. CPU0. UMD0. BDF 83:00.0 State: Foreign INTEL SSDPE2KE032T80 SN:BTLN962103HL3P2BGN 3.20TB Port 5:13. Slot 13. CPU0. UMD0. BDF 84:00.0 State: Foreign	View the drive details
Physical Drives Olon-supported or without	

**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<sup>®</sup> VROC SED Manager then enter System Revert. All secured drives are displayed.

# intel

```
Figure 2-32. Dashboard View – Re-Key
```

<1.0.0.1118> <enabled></enabled>	System Keys (Re-Key)'
<lnad1ed></lnad1ed>	
le-Key)	
F9=Reset to Defaults	F10=Save
	e-Key)

2. Select Execute System Re-Key.

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

Perform a change of a Physical Drives to R INTEL SSDPE2KX0800T80 INTEL SSDPE2KX0800T80 INTEL SSDPE2KE032T80 INTEL SSDPE2KX0800T80 INTEL SSDPE2KX0800T80 INTEL SSDPE2KE032T80 INTEL SSDPE2KE032T80 Execute System Re-Ker	all keys used by the UROC SED. eplace Keys (Re-Key): SN:BTLJ904600UN8P0HGN 8.00TB SN:BTLJ84860CBA8P0HGN 8.00TB SN:BTLJ904109PS3P2BGN 3.20TB SN:BTLJ904600EE8P0HGN 8.00TB SN:BTLJ904600EE8P0HGN 8.00TB SN:BTLJ90430EAN3P2BGN 3.20TB SN:BTLN905000KK3P2BGN 3.20TB	Execute the operation. Perform a change of all keys used by the UROC SED A configuration changing like hot-remove or hot-add during the operation is not recommended.
Back to Main Menu		

The following screen appears.

# intel.

#### Figure 2-34. Re-Key Completed Successfully Message

CALOCSEGRAGE CONFINEMENTATION NOME - THE CALIFUR DELAGE TRENCING ANOTHER TO FURN 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					
OnVrocSedDxeNotifu: HII alreadu started					
Exiting: OnVrocSedDxeNotify:125					
CVrocSedProxyChildDeviceInfo::DeviceIdentify [0x59E67580]: VMD idd: Success, loc					
ked 0					
CVrocSedProxyChildDe System Re-Key completed successfully. UMD 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) UROC SED - Key Identifiers		Intel(R) UROC SED - Key Identifiers		
	Addr +0 +1 +2 +3		Addr +0 +1 +2 +3	
(ey Identifier (s) :	0x00 02 36 B9 CF	Key Identifier(s):	0x00 88 86 38 5E	
02 36 B9 CF 52 50 04 E5 42 DF A6 F8 70 B8 9B>	0x04 52 50 04 E5	K88 BD 38 52 88 88 86 66 18 16 96 88 88 88 45>		
and day Martin Manua	UXUU 42 UF Hb FU	> Dack to Main Monu	0x00 3r b1 03 02	
ack to nain nenu	0x00 (0 B8 9B 3D 0-10 AP DE C7 03	P DACK CO HATH HERA	Av10 3R 90 10 R5	
	0x10 40 03 CT H3		0x14 CR 35 R7 R3	
	0x11 00 30 30 10 10		0x18 11 1D DE EB	
	0x1C 70 86 CF AD		0x1C 80 8C 59 75	
	0x20 76 94 B6 C0		0x20 3F 5F BA 40	
	0x24 5A D7 F0 C4		0x24 06 AB 1F 30	
	0x28 67 DD 30 97		0x28 A0 EF E6 D5	
	0x2C B2 86 90 EE		0x2C 3B 46 FC 53	
	0x30 C9 48 C5 10		0x30 8E 96 66 5D	
	Nore (D/d)		Nore (D	
		n		
-Move Highlight Esc	=Exit	x14=Move Highlight Es	c=Exit	

**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	^
(i) Information	8/18/2023 1:03:32 AM	Service Control Manager	7036	None	
Warning	8/18/2023 1:03:00 AM	iaVROC	4155	None	
(i) Information	8/18/2023 1:02:45 AM	Service Control Manager	7036	None	
(i) 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	
(i) Information	8/18/2023 1:01:49 AM	Service Control Manager	7036	None	
(i) Information	8/18/2023 1:01:45 AM	Service Control Manager	7036	None	
(i) Information	8/18/2023 1:01:18 AM	Service Control Manager	7036	None	
(i) 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, iaVRO	DC				×
General Detai	le.				
Delai	15				

### 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.

# intel.

#### Figure 3-2. Linux\* Warning

[ 107 597707] nume 10000-Ra-00 0: PCT TNT 4: no 6ST	
[ 113.518500] nume nume!: Shutdown timeout set to 15 seconds	
113 555511 nyme nyme1: 128/0/0 default/read/noll queues	
113 5897221 nymethi Read(0y2) A IAA & blocks Arress Denied (srt Av2 / sr Av86) DNR	
113 S807361 pritical target day numeral sector A nu BVA/(PEAN) flags BVA phys seg 1 prio class 2	
( 113 580744) Buffar t/D grow and unmaint, lagical block A some page road	
( 112.309744) burner 1/0 etror on dev nymestik, togical otoco v, devic page read	
[ 113.59770] RVMETRI, REDU( $x_2/y$ con 0, a blocks, Access Denieu (act $x_2/y$ so $x_30/$ DWA	
[ 113.369719] Critical Larger Error, devinnenta, securito o post, (new) riags oxo physiseg 1 prio Class 2	
( 113.509/03) Burnel 1/V erfor on dev nymestic, togical blocks , async page read	
[ 113.369000] NVMEINI: REAGOX2/ @ LAK 0, O DIOLKS, ALLESS DENIED (SELT 0X2 / SE 0X00) UNK	
[ 113.555003] Critical target error, dev nomental action of door.(new) ridge over phys_seg 1 prio class 2	
( 113.359606) Surfer 1/0 error on dev nymerni, togriat block 6, async page read	
[ 113.589822] NVMEINI: Read(0x2) @ LSA 0, 8 DIGCKS, ACCES Denied (SCC 0x2 / SC 0x80) DAR	
[ 113.589825] Critical target error, dev nymelni, sector 0 0 0x0:(ktau) Ttags 0x0 phys_seg 1 prio class 2	
1 113.589827] Butter 1/0 error on dev nymeini, togical block 0, async page read	
1 113.559843] nVmeini: Read(0X2) @ LBA 0, 8 Diocks, Access Denied (Stt 0X2 / Sc 0X86) DNR	
[ 113.589845] critical target error, dev numerni, sector 0 op exe:(READ) rtags exe phys_seg 1 prio class 2	
[ 113.589848] Buffer I/O error on dev nymeini, logical block 0, async page read	
[ 113.559864] nvmeini: Read(0x2) @ LBA 0, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR	
113.5595866] critical target error, dev nvmelnl, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 prio class 2	
[ 113.589869] Buffer I/O error on dev nymeini, logical block 0, async page read	
[ 113.589875] nvmeln1: unable to read partition table	
[ 113.595047] nvmeln1: Read(0x2) @ LBA 15628052992, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR	and the second
[ 113.595065] critical target error, dev numeln1, sector 15628052992 op 0x0:(READ) flags 0x80700 phys_seg 1 pr	io class 2
[ 113.595165] nvmeln1: Read(0x2) @ LBA 15628052992, 8 blocks, Access Denied (sct 0x2 / sc 0x86) DNR	
[ 113.595173] critical target error, dev numelni, sector 15628052992 op 0x0:(READ) flags 0x0 phys_seg 1 prio c	lass 2
[ 113.595179] Buffer I/O error on dev nvmeini, logical block 1953506624, async page read	
[root@localhost_joy]#	

§§