Hewlett Packard Enterprise

HPE Storage controllers and server: data at rest encryption overview

Contents

Introduction

The adoption of hybrid cloud, the Internet of Things (IoT), mobile networks, and artificial intelligence (AI) has opened businesses up to whole new categories of cyberthreats. Cybercriminals adapt rapidly, crafting more sophisticated, long-term attacks and penetrating server firmware at the code level. That's not to mention new government regulations and mounting pressure to improve service-level agreements (SLAs), which require security at the hardware level. There are many different solutions to address these challenges, including software and hardware solutions both at and above the server drive level.

To meet these challenges, HPE has developed solutions for advanced data security. HPE Storage controllers provide two approaches for data-at-rest encryption: self-encrypting drives (SED) and controller-based encryption (CBE).

Key management

Depending on the configuration, a controller may pass through or manage the encryption keys:

- **Host key management (HKM):** The keys are managed by third-party applications running in the operating system, such as SEDutil and are passed to the drive through the controller as normal SCSI commands.
- **Local key management (LKM):** The keys are stored and managed by the embedded controller firmware or HPE BIOS firmware allowing the data to be automatically unlocked after each reboot. Prior to Gen12 platforms TPM 2.0 is required for local (direct-attach) NVMe SED.
- **Remote key management (RKM):** The keys are stored by a third-party external key manager (EKM) also known as an RKM. The keys are retrieved using HPE iLO and BIOS firmware and used to unlock data. This is useful for securing data at a centralized location.

Self-encrypting drive (SED)

SED is another choice for data-at-rest encryption. It is an HDD or SSD that contains an Advanced Encryption Standard (AES) hardware encryption engine, which encrypts data at line rate as it is written to the storage media and provides access control by locking the drive once power is lost. The media encryption key (MEK) encrypts all the user data on the drive. It is stored encrypted on the drive and cannot be accessed by the user. The MEK is encrypted with a user password, also called a key encrypting key (KEK), which is used to unlock the drive and can be stored and managed by HKM, LKM, and RKM.

SED is ideal for customers who need their data protected with encryption. SEDs provide data-at-rest protection, which means that when power is lost (for example, when the server is turned off), the drive is locked, so if someone steals a drive from a server, they cannot read any of the data from that drive. SED performs at line rate, so it does not impact overall server performance, which is critical for customers in the financial service industry (FSI), healthcare, and the U.S. government sectors.

Mixing SED and non-SED is allowed within a server and a storage controller but not allowed within a volume. Figure 1. shows the configurations that can support SED with various key management modes.

Controller		Key Management		
		Host	Local	Remote
		3rd party key manager	Hosted by embedded firmware such as BIOS/ storage controller	3rd party remote key manager
Direct attached		✓	✓[2,4,5]	✓[2,5,8]
Intel®	VMD	✓[2]	X	X
	VROC	NA	X	✓[2,5,7,8]
MR Controller		✓[3]	✓	✓[8]
SR Controller		✓[1,6]	✓	✓[8]
NS Controller		NA	X	X

Note 1: HBA mode only
Note 2: NVMe only
Note 3: MR216 JBOD mode only
Note 4: TPM
Note 5: Hot-plugged drive requires reboot for key assignment
Note 6: Requiring user to take ownership with SID initiated.
Note 7: VROC License
Note 8: HPE iLO Adv License

Gen10
Gen10 Plus
Gen11
Gen12

Figure 1. Key Management

Controller-based encryption (CBE)

HPE Smart Array or SR storage controllers secure data before it's ever stored on a drive, using HPE Secure Encryption, a controller-based, enterprise-class data encryption solution that protects data at rest on RAID volumes. HPE Secure Encryption is compatible with all hard disk drives (HDDs) or solid-state drives (SSDs).

HPE Secure Encryption is available for both local and remote deployments. LKM mode provides a single-server deployment. RKM mode allows for central management of enterprise-wide deployment.

CBE is only supported on Gen10, Gen10 Plus and Gen11 platforms in RAID mode only. Refer to Figure 2. To learn more about CBE support, view the HPE Smart Array SR Secure Encryption QuickSpecs.

Controller	Key Management		
	Host	Local	Remote
	3rd party key manager	Hosted by embedded firmware such as BIOS/ storage controller	3rd party remote key manager
SR Gen11	X	✓ ●	✓ ● ●
SR Gen10+	X	✓ ●	✓ ● ●
SR Gen10[1,2]	X	✓ ●	✓ ● ●

Note 1: Most of the Gen10 SR controllers have a CBE FIPS listing
See "HPE Smart Array SR Encryption QuickSpecs" for FIPS support
Note 2: CBE with a remote key management server are not supported on Gen11 and later server utilizing Gen10 controller

● CBE Lic.
● iLO Adv Lic.

Figure 2. CBE enablement

Feature comparison between SED and CBE

The following are the feature comparison between SED and CBE.

Encryption type	SED	CBE
Description	SEDs provide hardware-based data encryption. All data that is committed to the media is encrypted with either a 128-bit or 256-bit key.	CBE encrypts all data as soon as it hits the controller, protecting your data from the PCIe bus all the way to the drive.
Drive selection	SED HDD/SSD	All HDD/SSD
License	HPE iLO Advanced License for RKM	Controller license per server HPE iLO Advanced License for RKM
Key management	Host, local, remote	Local, remote
Encryption point	Drive	Controller
Encrypted data	Drives	Controller cache, drive cable, drives
Encryption granularity	Full disk encryption (FDE) only	Per volume
Volume type	RAID or HBA/JBOD	RAID only
Drive replacement	Same as non-encrypted CPU attached drive (LKM/RKM) requires reboot	Same as non-encrypted
Controller replacement	Need controller credential	Need controller credential
Key rotation	Yes	Yes
Encrypting existing data	Yes	Yes

Important: Current CBE Users:

1) Gen12 platforms and above only support SED for data-at-rest encryption.
2) SED drives have their own unique SKUs from non-SED drives.
3) SED uses full disk encryption versus CBE which uses Logical Drive encryption.
4) In LKM mode with SED you no longer need to assign a key per logical volume.

FIPS validation

The Federal Information Processing Standards (FIPS) 140-2 and 140-3 are U.S. government standards that describe the encryption and security requirements that IT products should meet for sensitive, but unclassified, use. HPE works with our vendors to help ensure our solutions are validated with the latest FIPS standards in a timely fashion. For more information, visit NIST website.

CBE: To determine the FIPS validation status of HPE Smart Array SR Gen10 Controllers for CBE, refer to the HPE Smart Array SR Secure Encryption QuickSpecs.

SED: To determine the FIPS validation status of HPE SEDs, refer to the HPE Hard Disk Drive QuickSpecs, the HPE Solid-State Drive Selector or the HPE Solid State Drive QuickSpecs.

FIPS-140-3 requires SED password length to be at least 8 bytes, so while drives that were FIPS 140-2 validated would allow any password length, drives that are FIPS 140-3 validated will reject any password that is less than 8 bytes. It is recommended to create a password that is 32 bytes/characters in length.

Activation of SED features

The following are some guidelines for activating SED features for drives in the system and setting the SED key, depending on how the SED drives are attached and the key management the user plans to implement:

Key management	SEDs attached to	What you'll need	Related documentation
Host (HKM)	Direct attached MR controller SR controller Intel VMD	Third-party key manager (e.g., SEDutil)	Third-party key manager
Local (LKM)	Direct attached	UEFI System Utilities and TPM	hpe.com/support/UEFIGen10-UG-en hpe.com/support/UEFIGen11-UG-en hpe.com/support/UEFIGen12-UG-en
	MR controller	MRSA, StorCLI, or UEFI System Utilities	hpe.com/support/MRSA hpe.com/support/StorCLI hpe.com/support/MR-Gen10Plus-UG hpe.com/support/MR-Gen11-UG
	SR controller	SSA, SSACLI or UEFI System Utilities	hpe.com/support/ssa-ug hpe.com/support/ssacli-ug hpe.com/support/SR-Gen10-UG hpe.com/support/SR-Gen10Plus-UG hpe.com/support/SR-Gen11-UG
Remote (RKM)	Direct attached	HPE iLO supported third-party remote key manager HPE iLO Advanced License UEFI System Utilities	hpe.com/support/ilo5-ug-en hpe.com/support/ilo6-ug-en hpe.com/support/UEFIGen10-UG-en hpe.com/support/UEFIGen11-UG-en hpe.com/support/UEFIGen12-UG-en
	MR controller	HPE iLO supported third-party remote key manager HPE iLO Advanced License UEFI System Utilities	hpe.com/support/ilo5-ug-en hpe.com/support/ilo6-ug-en hpe.com/support/MR-Gen10Plus-UG hpe.com/support/MR-Gen11-UG
	SR controller	HPE iLO supported third-party remote key manager HPE iLO Advanced License SSA, SSACLI or UEFI System Utilities	hpe.com/support/ilo5-ug-en hpe.com/support/ilo6-ug-en hpe.com/support/ssa-ug hpe.com/support/ssacli-ug hpe.com/support/SR-Gen10-UG hpe.com/support/SR-Gen10Plus-UG hpe.com/support/SR-Gen11-UG
	Intel VROC	HPE iLO supported third-party remote key manager HPE iLO Advanced License UEFI System Utilities	hpe.com/support/ilo5-ug-en hpe.com/support/IntelVROC-Gen10Plus-Win-UG hpe.com/support/VROC-Gen11-UG

HPE MR storage controllers

The HPE MR storage controllers are a family of tri-mode controllers ideal for maximizing performance while supporting advanced RAID levels. This controller operates in mixed mode, which combines RAID and JBOD operations simultaneously.

Key management support

HPE MR storage controllers support SED in HKM, LKM, and RKM modes. When booting up, the security key is retrieved from the key manager to unlock the drive. This action protects the drives and system against data theft.

Enabling SED key management

LKM

You can enable SED drive security for LKM using the HPE MR Storage Administrator, StorCLI tool, and configuration utility in UEFI System Utilities. You must provide a controller-wide security key identify and security key. While booting up, the security key stored in the controller is used to unlock the drive. Whenever the drive is powered down, the security-enabled drive data encryption key is locked. This action protects the drives against data theft.

- UEFI System Utilities: See "Enabling Drive Security" in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.
- MRSA: See "Enabling Drive Security" in the HPE MR Storage Administrator User Guide.
- StorCLI: See "Controller Security Commands" in the HPE StorCLI User Guide.
- Redfish: Available starting with 5.300.03-4116 see HPE Storage Controllers – Management overview "Storage" section for redfish management commands.

RKM

You can enable SED drive security for RKM using the configuration utility in UEFI System Utilities.

The configuration utility in UEFI System Utilities works with HPE iLO key manager to create the security key identify and security key in the remote key manager server. HPE iLO key manager needs to be configured before enabling RKM in the configuration utility. Whenever the drive is powered down, the security-enabled drive data encryption key is locked.

- UEFI System Utilities: See "Enabling Drive Security" in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.
- StorCLI: Enable RKM by StorCLI is supported from 007.2207.0000.0000. Use "storcli/cx set securitykey useekms" to enable RKM. Reboot is required for the change to take effect. Command details can be found by "storcli help securitykey."
- Redfish: available starting with 5.300.03-4116 see HPE Storage Controllers – Management overview "Storage" section for redfish management commands.
- Please refer to "Supported key managers" section in HPE iLO 5 User Guide and HPE iLO 6 User Guide and "Encryption and key management" section in HPE Compute Security Reference Guide for details on how to set up RKM in HPE iLO.

Maintenance

Drive replacement

Secured drive replacement is the same as normal, unsecured drive replacement. For more details and information, see the "Replace drive" section in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.

Controller replacement

If some or all the drives managed by the controller being replaced are encrypted, you must reconfigure the replacement controller with the same settings and key management mode you used for the controller you are replacing.

Server replacement

If you retain the same controller and physical disks, then there are no encryption-related tasks to complete. If Remote Key Management Mode is in use, the previous HPE iLO configuration for key management must be applied to the new server.

Importing foreign security enabled drives

LKM

For HPE MR storage controllers, the importing volumes in the foreign security-enabled drives remain offline until user intervention is taken.

- UEFI System Utilities: See "Importing secured foreign drive" in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.
- MRSA: See "Importing or Clearing a Foreign Configuration—Security-Enabled Drives" in the HPE MR Storage Administrator User Guide.
- StorCLI: See "Foreign Configurations Commands" in the HPE StorCLI User Guide.

RKM

It is possible to import a foreign drive within the same controller family. In RKM mode, drives automatically import when the associated key is present on the ESKM. A reboot will be required for the controller to retrieve the associated key to unlock SEDs and import drives automatically.

Key rotation

Key rotation refers to retiring an encryption key and generating a new one. Rotating keys on a regular basis helps meet industry standards and cryptographic best practices.

LKM

Key rotation is initiated by the controller management tool.

- UEFI system utilities (requires reboot): See the "Changing Drive Security settings" section in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.
- MRSA (no reboot required): See the "Changing Drive Security settings" section in the HPE MR Storage Administrator User Guide.
- StorCLI (no reboot required): See "Controller Security Commands" in the HPE StorCLI User Guide.

RKM

Key rotation operation is supported only in UEFI system utilities.

- UEFI system utilities (requires reboot): See the "Changing Drive Security settings" section in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.

Drive secure erase/PSID revert

SED PSID revert is not supported. Use Cryptographic Erase to erase the SED that is owned by the controller.

- UEFI system utilities: See the "Sanitizing an Unconfigured Good drive" section in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.
- MRSA: See the "Erasing a Drive Securely" section in the HPE MR Storage Administrator User Guide.
- StorCLI: Please use "Drive Secure Erase Commands" in HPE StorCLI User Guide.
- Redfish: see HPE Storage Controllers – Management overview "Drive" section for redfish management commands.

LKM to RKM transition

MR Gen10 Plus and Gen11 controllers can be transitioned from LKM to SEKM mode if your iLO system has an advanced license.

- UEFI: See "Changing drive security key management mode" in in the HPE MR Gen10 Plus Controller User Guide and HPE MR Gen11 Controller User Guide.
- Redfish: Available starting with 5.300.03-4116 see HPE Storage Controllers – Management overview "Storage" section for redfish management command.

RKM to LKM transition

Not supported.

HPE Smart Array SR storage controllers

HPE SR storage controller portfolio provides enterprise-class storage performance, reliability, security, and efficiency needed to address your evolving data storage needs.

Key management support

HPE SR storage controllers support controller-based encryption on RAID volumes in LKM and RKM mode and SED drives in HKM and LKM mode. User can enable either CBE or SED key management.

Enabling SED key management

Please refer to the "Self-Encrypting Drive" section in HPE Smart Array SR Gen10 Controller User Guide, HPE SR Gen10 Plus Controller User Guide and HPE SR Gen11 Controller User Guide for SED support details.

LKM

You can enable SED key management for LKM using the SSA/SSACLI controller configuration utilities.

- SSA: See "SED Based Encryption Setup" section in the HPE Smart Storage Administrator GUI User Guide
- SSACLI: See "SED Based Encryption Commands" section in the HPE Smart Storage Administrator CLI User Guide

RKM

HPE iLO key manager interface needs to be configured before enabling RKM in the controller configuration utility. Please refer to "Supported key managers" section in HPE iLO 5 User Guide and HPE iLO 6 User Guide and "Encryption and key management" section in HPE Compute Security Reference Guide for details on how to set up HPE iLO.

You can enable SED key management for RKM using the SSA/SSACLI controller configuration utilities.

- SSA: See "SED Based Encryption Setup" section in the HPE Smart Storage Administrator GUI User Guide
- SSACLI: See "SED Based Encryption Commands" section in the HPE Smart Storage Administrator CLI User Guide

Enabling CBE key management

Please refer to the "CBE Setup" section of the HPE Smart Storage Administrator GUI User Guide or "Controller-Based Encryption Commands" section of the HPE Smart Storage Administrator CLI User Guide for details on how to set up LKM/RKM.

LKM

You can enable CBE drive security for LKM using the SSA/SSACLI/UEFI controller configuration utilities. You must provide a password and master key. While booting up, the master key stored in the controller is used to decrypt the logical drive data.

RKM

HPE iLO key manager interface needs to be configured before enabling RKM in the controller configuration utility. The controller configuration utility (SSA/SSACLI/UEFI) configures RKM including the security key identifier.

Please refer to "Supported key managers" section in HPE iLO 5 User Guide and HPE iLO 6 User Guide "Encryption and key management" section in HPE Compute Security Reference Guide for details on how to set up HPE iLO.

Maintenance

Drive replacement

Secured drive replacement is the same as normal, unsecured drive replacement. For more information, see the "Array Transformations" section in the HPE Smart Array SR Gen10 Controller User Guide, HPE SR Gen10 Plus Controller User Guide and HPE SR Gen11 Controller User Guide.

Controller replacement

If some or all the drives managed by the controller being replaced are encrypted, you must reconfigure the replacement controller with the same settings and key management mode you used for the controller you are replacing.

Server replacement

If you retain the same controller and physical disks, then there are no encryption-related tasks to complete. If Remote Key Management Mode is in use, the previous HPE iLO configuration for key management must be applied to the new server.

Importing foreign security enabled drives

LKM

The HPE Storage administrator tool can be used to supply the passphrase for the imported drives in LKM mode. The importing volumes in the foreign security-enabled drives remain offline until user intervention is taken. It is possible to import a foreign drive within the same controller family.

For CBE,

- SSA: See "Importing Drive Sets in Local Key Management Mode" section in the HPE Smart Storage Administrator GUI User Guide
- SSACLI: See "CBE Support Commands" section in the HPE Smart Storage Administrator CLI User Guide

For SED,

- SSA: See "Importing Foreign SED" section in the HPE Smart Storage Administrator GUI User Guide
- SSACLI: See "Managed SED Support Commands" section in the HPE Smart Storage Administrator CLI User Guide

RKM

It is possible to import a foreign drive within the same controller family.

For CBE,

- Drives are automatically unlocked and imported when the associated key is present on the ESKM for Gen10 and Gen10 Plus controllers, no reboot is needed. For Gen11 controllers, a reboot is needed to retrieve the key.

For SED,

- Once the system is rebooted the drives are automatically unlocked and imported for Gen11 controllers when the associated key is present on the ESKM.

Key Rotation

Key rotation refers to retiring an encryption key and generating a new one. Rotating keys on a regular basis helps meet industry standards and cryptographic best practices. If the Gen10 or Gen10 Plus controller is in a supported generation of server this can be done at runtime. For Gen11 controllers a reboot is needed.

CBE LKM and RKM

- SSA: See "Working with Keys" section in the HPE Smart Storage Administrator GUI User Guide
- SSACLI: see "Encryption key commands" section in the HPE Smart Storage Administrator CLI User Guide

SED LKM and RKM

- SSA: See "Changing Master Key" section in the HPE Smart Storage Administrator GUI User Guide
- SSACLI: See "Change the SED Encryption Master Key" section in the HPE Smart Storage Administrator CLI User Guide

Drive secure erase/PSID revert

Data erasure for HPE SR storage controllers is the same as normal drive erasure process. SED PSID revert is supported using SSA/SSACLI/UEFI.

- SSA: See "Erasing a drive" and "Revert to the Original Factory State" section in the HPE Smart Storage Administrator GUI User Guide
- SSACLI: See "Erasing a physical drive" and "Revert an SED to its OFS Using PSID" section in the HPE Smart Storage Administrator CLI User Guide
- Redfish: See HPE Storage Controllers – Management overview "Drive" section for redfish management commands

Local NVMe SED (Direct-Attached NVMe SED)

The local NVMe SED feature is supported by UEFI System Utilities User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, HPE Synergy and UEFI System Utilities User Guide for HPE ProLiant Gen11 Servers and HPE Synergy.

Key management support

Local NVMe drives support SED in LKM and RKM modes. HKM is supported for both SATA and NVMe SED.

Enabling SED key management

LKM

You can enable SED drive security for LKM using the configuration utility in UEFI System Utilities. You must provide a security key. While booting up, the security key stored locally on the server is used to unlock the drive. Whenever the drive is powered down, the security-enabled drive data encryption key is locked. This action protects the drives against data theft.

- UEFI System Utilities: See the "Configuring SED Drives for local and remote key management" section in the following documents:
  - UEFI System Utilities User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen11 Servers and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen12 Servers and HPE Synergy

RKM

The configuration utility in UEFI System Utilities works with HPE iLO key manager to create the security key in the remote key manager server. HPE iLO key manager needs to be configured before enabling RKM in the configuration utility. Whenever the drive is powered down, the security-enabled drive data encryption key is locked.

- UEFI System Utilities: See the "Configuring SED Drives for local and remote key management" section in the following documents:
  - UEFI System Utilities User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen11 Servers and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen12 Servers and HPE Synergy
- Please refer to "Supported key managers" section in HPE iLO 5 User Guide and HPE iLO 6 User Guide and "Encryption and key management" section in HPE Compute Security Reference Guide for details on how to set up RKM in HPE iLO.

Maintenance

Drive replacement

It is required to reconfigure the SED drive security for the replaced drive.

Controller replacement

Controller replacement is not applicable. Local NVMe SED is supported in system ROM.

Server replacement

If you retain the same physical disks, the previous configuration for key management must be applied to the new server.

Importing foreign security enabled drives

LKM

Device encryption migration process is required. Use "Device Encryption Export option" from the source server, you will need a "transient password" for the key migration. On the target server, use "Device Encryption Recovery option," select the keys file, and input the transient password.

- UEFI System Utilities: leverage the steps from "Changing HPE Persistent Memory module passwords" in the following documents:
  - UEFI System Utilities User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen11 Servers and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen12 Servers and HPE Synergy

RKM

In RKM mode, drives automatically import when the associated key is present on the ESKM. A reboot will be required to retrieve the associated key to unlock SED and import drives automatically.

Key rotation

Key rotation refers to retiring an encryption key and generating a new one. Rotating keys on a regular basis helps meet industry standards and cryptographic best practices.

LKM

The encryption key is stored locally on the server. For platforms prior to Gen12 the HPE TPM 2.0 must be installed

to view and select this setting. For Gen12 the encryption keys are stored in the iLO secure enclave.

See the steps from "Changing HPE Persistent Memory module passwords" section in the following documents:

- UEFI System Utilities User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, and HPE Synergy
- UEFI System Utilities User Guide for HPE ProLiant Gen11 Servers and HPE Synergy
- UEFI System Utilities User Guide for HPE ProLiant Gen12 Servers and HPE Synergy

RKM

Key rotation in RKM mode is not supported.

Drive secure erase/PSID revert

Drive secure erase is performed using One Button Secure Erase (OBSE). If an SED's internal key or drive access password is lost or deleted, the drive data becomes permanently inaccessible and unreadable. The drive is unusable in this state but may be reset and reformatted so that it can be repurposed. The drive can be manually reverted to the unowned state by using its Physical Security ID (PSID).

- UEFI System Utilities: Server Security > Device Encryption Options > Device Encryption Migration Options > Device Encryption Recovery Options > Revert OPAL drives to factory default.

Intel VROC

Intel Virtual RAID on CPU (VROC) is an enterprise RAID solution, specifically designed for NVMe SSDs connected directly to the CPU.

Key management support

Intel VROC supports NVMe SED in RKM mode only. HKM mode is supported for VMD NVMe SED.

Enabling SED key management

LKM

Not supported.

RKM

Intel VROC supports SED RKM and allows you to generate one system key per drive from HPE iLO using an external key manager.

- UEFI System Utilities: See the "Setting up the security and encryption configurations" section in the Intel Virtual RAID on CPU for HPE Gen10 Plus User Guide and Intel Virtual RAID on CPU for HPE User Guide.
- Please refer to "Supported key managers" section in HPE iLO 5 User Guide and HPE iLO 6 User Guide and "Encryption and key management" section in HPE Compute Security Reference Guide for details on how to set up RKM in HPE iLO.

Maintenance

Drive replacement

Drive replacement is the same as a normal drive, however, a reboot is required for VROC to provision the SED. It is recommended to configure hot spare, so when an array member drive fails, it will be automatically replaced and start rebuilding.

- For Gen10 plus server, please refer to the "Drive states and recovery" section in the Intel Virtual RAID on CPU for HPE Gen10 Plus User Guide for failure drive replacement.
- For Gen11 server, please refer to "Replace Drive" and "Drive Rebuild" sections in the Intel Virtual RAID on CPU for HPE User Guide.

Controller replacement

Controller replacement is not applicable. VROC is supported in system ROM.

Server replacement

If you retain the same physical disks, the previous configuration for key management must be applied to the new server.

Importing foreign security enabled drives

RKM

It is possible to import a foreign array from another server's VROC. In RKM mode, drives will be automatically imported when the associated key is present on the ESKM. It is recommended to shut off the system, insert drives and then power on the system. Make sure all the array member drives are inserted, VROC will retrieve the associated key to unlock SED and import drives automatically.

- For Gen10 plus server, please refer to the "Intel VROC NVMe hot insert" section in Intel Virtual RAID on CPU for HPE Gen10 Plus User Guide for drive hot insert limitation.
- For Gen11 server, please refer to the "Foreign configuration import" section in the Intel Virtual RAID on CPU for HPE User Guide.

Key rotation

Key rotation refers to retiring an encryption key and generating a new one. Rotating keys on a regular basis helps meet industry standards and cryptographic best practices.

RKM

The encryption key is stored on a remote key server. HPE iLO must be enrolled in and connected to a remote key manager to view and select this setting. Please see "Replacing system keys" in Intel Virtual RAID on CPU for HPE Gen10 Plus User Guide and Intel Virtual RAID on CPU for HPE User Guide.

Drive secure erase/PSID revert

VROC supports SED Drive secure erase and PSID revert. Both operations are performed using UEFI System Utilities.

- For Drive erase, see "Erasing drive securely" session in Intel Virtual RAID on CPU for HPE Gen10 Plus User Guide and Intel Virtual RAID on CPU for HPE User Guide.
- For PSID revert, see "Reverting PSID" session in Intel Virtual RAID on CPU for HPE Gen10 Plus User Guide and Intel Virtual RAID on CPU for HPE User Guide.
- Redfish: HPE Storage Controllers – Management overview "Drive" section for redfish management commands

Glossary

- Advanced Encryption Standard (AES)
- Controller-based encryption (CBE)
- Enterprise Secure Key Manager (ESKM)
- Federal Information Processing Standards (FIPS)
- Hard disk drive (HDD)
- Host key management (HKM)
- Key encrypting key (KEK)
- Local key management (LKM)
- Media encryption key (MEK)
- MegaRAID (MR)
- National Institute of Standards and Technology (NIST)
- ROM-based setup utility (RBSU)
- Remote key management (RKM)
- Self-encrypting drive (SED)
- SmartRAID (SR)
- Solid-state drive (SSD)
- Trusted Platform module (TPM)

- Physical Security (ID)entification (PSID)

Resources

- SSD
  - HPE SSD QuickSpecs
  - HPE Solid-State Drive Selector
- SED
  - HPE Hard Disk Drives QuickSpecs
  - HPE Solid-State Drive Selector
- SR Controller
  - HPE SR Smart Storage Administrator GUI User Guide
  - HPE SR Smart Storage Administrator CLI User Guide
  - HPE Smart Array SR Gen10 Controller User Guide
  - HPE SR Gen10 Plus Controller User Guide
  - HPE SR Gen11 Controller User Guide
  - HPE Secure Encryption QuickSpecs
- MR Controller
  - HPE MR Storage Administrator User Guide
  - HPE StorCLI User Guide
  - HPE MR Gen10 Plus Controller User Guide
  - HPE MR Gen11 Controller User Guide
- CPU Direct Attached
  - UEFI System Utilities User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen11 Servers and HPE Synergy
  - UEFI System Utilities User Guide for HPE ProLiant Gen12 Servers and HPE Synergy
- Intel VROC
  - Intel Virtual RAID on CPU for HPE Gen10 Plus User Guide, Microsoft Windows edition: hpe.com/support/IntelVROC-Gen10Plus-Win-UG
  - Intel Virtual RAID on CPU for HPE User Guide: hpe.com/support/VROC-Gen11-UG

a50006629ENW, Rev. 4