Hewlett Packard Enterprise

Self-encrypting drives

Contents

Purpose

The purpose of this document is to provide answers to questions that are frequently asked regarding self-encrypting drives (SEDs).

Overview

Q: What is a self-encrypting drive (SED)? How will the user manage keys (that is, passwords) for SED?

A: A self-encrypting drive (SED) 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) is used to encrypt all the user data on the drive. It is stored encrypted on the drive and cannot be accessed by the user. It is encrypted with the key encrypting key (KEK) (that is, user password) that is used to unlock the drive and can be stored and managed by three management types:

- **Host Key Management (HKM):** OS utility manages keys
- **Local Key Management (LKM):** Server-based key management
- **Remote Key Management (RKM):** Enterprise key managers for auditable high-availability business-critical keys

Q: What is necessary to enable SED? What are the viable configurations that can support SED?

A: The minimum requirement is to get a SED drive. A controller is optional and only a hard requirement for SAS SED drives. The following are the configurations that can support SED with various key management:

Controller	Key management: Host (Third-party key manager)	Key management: Local (Hosted by embedded firmware such as BIOS/storage controller)	Key management: Remote (Third-party remote key manager)
Direct attached	✓	✓[2, 5] ●	✓[2, 5] ●
Intel® VMD	✓[2, 4]	X	X
Intel® VROC	NA	X	✓[2, 4, 5] ● ●
MR Gen11	✓[3]	✓	✓ ●
MR Gen10+	✓[3]	✓	✓ ●
SR Gen11	✓[1, 6]	✓	✓ ●
SR Gen10+	✓[1, 6]	✓	✓ ●
SR Gen10	✓[1, 6]	✓	✓ ●
NS Gen10+	NA	X	X

● VROC License
● HPE iLO Adv. License
● TPM

[1] HBA mode only
[2] NVMe only
[3] MR216 JBOD mode only
[4] Support on Gen10+/Gen11 only
[5] Hot-plugged drive requires reboot for key assignment
[6] Requiring user to take ownership with SID initiated

Figure 1. SED enablement

Q: Which controllers support SEDs?

A: Currently, the SR/MR controllers listed in the following can support SED.

SR controllers:

Gen10:

- 830824-B21 HPE Smart Array P408i-p SR Gen10 (8 Internal Lanes/2GB Cache) 12G SAS PCIe Plug-in Controller
- 804331-B21 HPE Smart Array P408i-a SR Gen10 (8 Internal Lanes/2GB Cache) 12G SAS Modular Controller
- 869081-B21 HPE Smart Array P408i-a SR Gen10 (8 Internal Lanes/2GB Cache) 12G SAS Modular LH Controller
- 804405-B21 HPE Smart Array P408e-p SR Gen10 (8 External Lanes/4GB Cache) 12G SAS PCIe Plug-in Controller
- 804394-B21 HPE Smart Array E208i-p SR Gen10 (8 Internal Lanes/No Cache) 12G SAS PCIe Plug-in Controller
- 804326-B21 HPE Smart Array E208i-a SR Gen10 (8 Internal Lanes/No Cache) 12G SAS Modular Controller
- 869079-B21 HPE Smart Array E208i-a SR Gen10 (8 Internal Lanes/No Cache) 12G SAS Modular LH Controller
- 804398-B21 HPE Smart Array E208e-p SR Gen10 (8 External Lanes/No Cache) 12G SAS PCIe Plug-in Controller
- 804338-B21 HPE Smart Array P816i-a SR Gen10 (16 Internal Lanes/4GB Cache/SmartCache) 12G SAS Modular Controller
- 869083-B21 HPE Smart Array P816i-a SR Gen10 (16 Int Lanes/4GB Cache/SmartCache) 12G SAS Modular LH Controller

Gen10 Plus:

- P04220-B21 Microchip SmartRAID SR932i-p x32 Lanes 8GB Wide Cache NVMe/SAS 24G Controller for HPE Gen10 Plus
- P12688-B21 Microchip SmartRAID SR416i-a x16 Lanes 4GB Cache NVMe/SAS 24G Controller for HPE Gen10 Plus

Gen11:

- P47184-B21 HPE SR932i-p Gen11 x32 Lanes 8GB Wide Cache PCI SPDM Plug-in Storage Controller

MR controllers:

Gen10 Plus:

- P26279-B21 Broadcom MegaRAID MR416i-a x16 Lanes 4GB Cache NVMe/SAS 12G Controller for HPE Gen10 Plus
- P06367-B21 Broadcom MegaRAID MR416i-p x16 Lanes 4GB Cache NVMe/SAS 12G Controller for HPE Gen10 Plus
- P26325-B21 Broadcom MegaRAID MR216i-a x16 Lanes without Cache NVMe/SAS 12G Controller for HPE Gen10 Plus
- P26324-B21 Broadcom MegaRAID MR216i-p x16 Lanes without Cache NVMe/SAS 12G Controller for HPE Gen10 Plus

Gen11:

- P47777-B21 HPE MR416i-p Gen11 x16 Lanes 8GB Cache PCI SPDM Plug-in Storage Controller
- P47781-B21 HPE MR416i-o Gen11 x16 Lanes 8GB Cache OCP SPDM Storage Controller
- P47785-B21 HPE MR216i-p Gen11 x16 Lanes without Cache PCI SPDM Plug-in Storage Controller
- P47789-B21 HPE MR216i-o Gen11 x16 Lanes without Cache OCP SPDM Storage Controller
- P58335-B21 HPE MR408i-o Gen11 x8 Lanes 4GB Cache OCP SPDM Storage Controller

Q: How do I activate the SED feature for the drives in the system? What will be the interface for setting the SED key on HPE ProLiant servers?

A: The following are some guidelines 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	Third-party key manager (for example, SEDutil)	Third-party key manager
	SR controller		
	MR controller		
	Intel VMD		
Local (LKM)	Direct attached	UEFI System Utilities and TPM	hpe.com/support/UEFIGen10-UG-en hpe.com/support/UEFIGen11-UG-en
	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
	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
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
	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
	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

Q: How are keys managed when using a controller?

A: Depending on the configuration, a controller may pass through or manage the key encrypting keys:

- **Host:** The keys are managed by the OS tool and are passed through the controller as normal SCSI commands.
- **Local:** If the controller is attached, it stores and manages the SED keys.
- **Remote:** If the controller is attached, it receives the keys via the BIOS and HPE iLO, but they are stored on the remote key management server.

Q: What is the difference between digitally signed FW, SED, and FIPS?

A:

- **Digitally signed FW:** A technology that assists in the secure update of firmware, ensuring that the firmware has not been tampered with since being built.
- **SED:** A self-encrypting drive is a drive that contains an 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.

- **FIPS:** Federal Information Processing Standards (FIPS) are standards and guidelines for federal computer systems that are developed by the National Institute of Standards and Technology (NIST) per the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. FIPS validated drives are tested by a third-party NIST-approved lab to ensure that they use NIST-approved cryptographic algorithms (for example, AES) and hashes in addition to meeting a set of testable cryptographic and security requirements.

Q: How do I activate the FIPS capability for the drives in the system?

A: For drives, no FIPS mode needs to be activated in the system. FIPS is a certification for SED drives. Hewlett Packard Enterprise offers FIPS validated drives, which are listed on the National Institute of Standards and Technology (NIST) website. Below is one example of HPE SED FIPS HDD which has been posted on NIST website. csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2796

Q: Will SEDs be offered in Gen10, Gen10 Plus and Gen11 platforms?

A: Yes. Refer to Figure 1.

Q: Do I need a SED?

A: A 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 (that is, 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 key customers in the FSI, healthcare, and the U.S. government sectors.

Q: Can a customer mix use the SEDs and non-SEDs?

A: Mixing SED and non-SED is allowed within a server and a RAID controller. It's not allowed within a volume.

Learn more at

HPE storage controllers and server: data encryption overview

Chat now (sales)

a50004902ENW, Rev. 3

Hewlett Packard Enterprise