HX Security Encryption FAQ

As of HXDP 5.01b, HyperFlex offers a software-based solution using Intersight Key Manager for systems that either do not support hardware-based encryption or for users that desire this functionality over hardware solutions. This FAQ focuses only on SED based hardware solutions for HX encryption. See the administration documents or whitepaper(s) for information on software-based encryption.

Bias Statement

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

1.0 Why Cisco for Security and HX Encryption

Q 1.1: What processes are in place for secure development?
A 1.1: Cisco Servers adhere to Cisco Secure Development Lifecycle (CSDL):

- Cisco provides processes, methodologies, framework to develop embedded security on Cisco servers, not just an overlay
- Dedicated Cisco team for threat modeling/static analysis on UCS Product Portfolio
- Cisco Advanced Security Initiative Group (ASIG) performs proactive penetration testing to understand how threats come in and fix issues by enhancing HW & SW through CDETS and engineering
- Dedicated Cisco team to test and handle outbound vulnerability and communicate as security advisors to customers
- All underlying products go through product security baseline requirements (PSB) which governs security standards for Cisco products
- Cisco performs Vulnerability/Protocol robustness testing on all UCS releases

Q 1.2: Why are SEDs important?
A 1.2: SEDs are used for data-at-rest encryption and are a requirement for many, if not all, federal, medical, and financial institutions.

2.0 General Information Overview

Q 2.1: What are SEDs?
A 2.1: SED (Self-Encrypting Drives) have special hardware that encrypts incoming data and decrypts outgoing data in real-time.

Q 2.2: What is the scope of encryption on HX?
A 2.2: Encryption on HX is currently implemented in hardware for data at rest only using encrypted drives (SEDs). HX encryption is cluster-wide. Individual VM encryption is handled by 3rd party software such as Hytrust or Vormetric's transparent client and is outside the scope of HX responsibilities. HX also supports the use of VMware's native VM encryption introduced in vSphere 6.5. Use of a VM encryption client on top of HX SED

based encryption will result in double encryption of the data. HX replication is not encrypted and relies on trusted networks or encrypted tunnels deployed by the end user.

Q 2.3: What compliance standards are met with HX encryption?
A 2.3: HX SED encrypted drives meet FIPS 140-2 level 2 standards from the drive manufacturers. HX Encryption on the platform meets FIPS 140-2 level 1 standards.

Q 2.4: Do we support both HDD and SSD for encryption?
A 2.4: Yes we support both HDD and SSD SEDs from Micron.

Q 2.5: Can an HX cluster have encrypted and non-encrypted drives at the same time?
A 2.5: All nodes in cluster must be uniform (SEDs or non-SEDs)

Q 2.6: What keys are in use for a SED and how are they used?
A 2.6: There are two keys in use for each SED. The Media Encryption Key (MEK) also called the Disk Encryption Key (DEK), controls encryption and decryption of the data to the disk and is secured and managed in hardware. The Key Encryption Key (KEK) secures the DEK/MEK and is maintained in either a local or remote keystore.

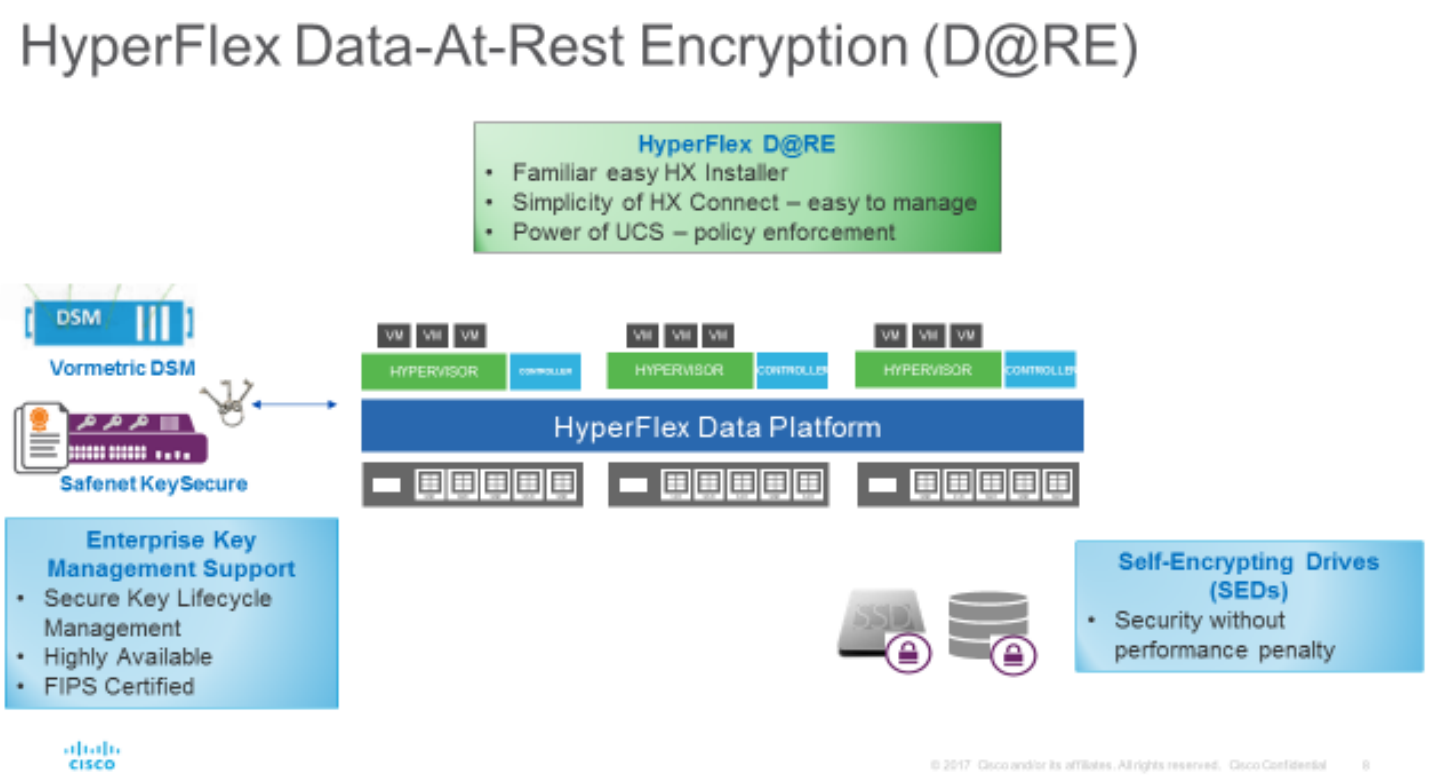
Q 2.7: Are the keys ever present in memory?
A 2.7: Encryption keys are never present in node memory

Q 2.8: How is performance impacted by the encryption/decryption process?
A 2.8: Disk encryption/decryption is handled in the drive hardware. Overall system performance is not affected and is not subject to attacks targeting other components of the system

Q 2.9: Other than encryption at rest, what are other reasons to use SEDs?
A 2.9: SEDs can reduce drive retirement and redeployment costs through instantaneous cryptographic erasure. They also serve to comply with government or industry regulations for data privacy. Another advantage is the reduced risk of disk theft and node theft since the data, once the hardware is removed from the ecosystem, is unreadable.

Q2.10: What happens with deduplication and compression with SEDs? What happens with 3rd party software based encryption?
A2.10: Deduplication and compression with SEDs on HX is maintained since the data at rest encryption takes place as a last step in the write process. Deduplication and compression have already taken place. With 3rd party software-based encryption products, the VMs manage their encryption and pass encrypted writes to the hypervisor and subsequently HX. Since these writes are already encrypted, they do not get deduplicated or compressed. HX Software Based Encryption (in the 5.x codeline) will be a software encryption solution that is implemented in the stack after write optimizations (deduplication and compression) have occurred so the benefit will be retained in that case.

The figure below is an overview of the implementation of SED with HX.



3.0 Drive Details

Q 3.1: Who manufactures the encrypted drives that are used in HX?
A 3.1: HX uses drives manufactured by Micron:

Micron specific documents are linked in the supporting documents section of this FAQ.

Q 3.2: Do we support any SEDs that are not FIPS compliant?
A 3.2: We also support some drives which are non-FIPS, but support SED (TCGE).

Q 3.3: What is the TCG?
A 3.3: TCG is the Trusted Computing Group, which creates and manages the specifications standard for encrypted data storage

Q 3.4: What is considered enterprise class security when it comes to SAS SSDs for the data center? What specific features do these drives have that ensure security and protect against attack?

Figure 1: Hyperflex SED Implementation

A 3.4: This list summarizes the enterprise class features of the SEDs used in HX and how they relate to the TCG standard.

1. Self-encrypting drives (SEDs) provide strong security for data at rest on your SED, preventing unauthorized data access. The Trusted Computing Group (TCG) has developed a **list of the features and benefits** of self-encrypting drives for both HDDs and SSDs. The TCG provides a standard that is called the TCG Enterprise SSC (Security Subsystem Class) and is focused on data at rest. This is a requirement for all SEDs. The spec applies to data storage devices and controllers which operate in enterprise storage. The list includes:

    - **Transparency:** No system or application modifications required; encryption key generated by the drive itself, using an on-board true random number generator; drive is always encrypting.
    - **Ease of management:** No encryption key to manage; software vendors exploit standardized interface to manage SEDs, including remote management, pre-boot authentication, and password recovery
    - **Disposal or re-purposing cost:** With an SED, erase on-board encryption key
    - **Re-encryption:** With SED, there is no need to ever re-encrypt the data
    - **Performance:** No degradation in SED performance; hardware-based
    - **Standardization:** Whole drive industry is building to the TCG/SED Specifications
    - **Simplified:** No interference with upstream processes

2. SSD SEDs provide is the ability to cryptographically erase the drive. This means that a simple authenticated command can be sent to the drive to change the 256-bit encryption key stored on the drive. This ensures that the drive is wiped clean and there is no data remaining. Even the original host system can't read the data, so it absolutely will be unreadable by any other system. The operation only takes a couple seconds, as opposed to the many minutes or even hours that it takes to perform an analogous operation on an unencrypted HDD and avoids the cost of expensive HDD de-gaussing equipment or services.
3. FIPS (Federal Information Processing Standard) 140-2 is a U.S. government standard that describes the encryption and related security requirements that IT products should meet for sensitive, but unclassified, use. This is often a requirement for government agencies and companies in the financial services and health care industries are adopting is as well. An SSD that is FIPS-140-2 validated uses strong security practices including approved encryption algorithms. It also specifies how individuals or other processes must be authorized in order to utilize the product, and how modules or components must be designed to securely interact with other systems. In fact, one of the requirements of a FIPS-140-2 validated SSD drive is that it is a SED. Bear in mind that although TCG is not the only way to get a certified encrypted drive, the TCG Opal and Enterprise SSC specifications provide us a stepping stone to FIPS validation.
4. Another essential feature is Secure Downloads and Diagnostics. This firmware feature protects the drive from software attacks through a digital signature that is built into the firmware. When downloads are needed, the digital signature prevents unauthorized access to the drive, preventing counterfeit firmware from being loaded to the drive.

4.0 Hyperflex install with SEDs

Q 4.1: How does the installer handle a SED deployment? Are there any special checks?
A 4.1: The installer communicates with UCSM and ensures that system firmware is correct and supported for the detected hardware. Encryption compatibility is checked and enforced (e.g., no mixing of SED and non-SED).

Q 4.2: Is the deployment any different otherwise?

A 4.2: The install is similar to a regular HX install, however, custom workflow not supported for SEDs. This operation requires UCSM credentials for the SEDs too.

Q 4.3: How does licensing work with encryption? Is there anything extra that needs to be in place?
A 4.3: SED hardware (ordered from factory, not retrofit) + HXDP 2.5 + UCSM (3.1(3x)) are the only things needed to enable encryption with key management. There is no additional licensing outside of the base HXDP subscription required in the 2.5 release.

Q 4.4: What happens when I have a SED system that has drives that are no longer available? How can I expand this cluster?
A 4.4: Whenever we have any PID that is end-of-life from our suppliers, we have a replacement PID that is compatible with the old PID. This replacement PID can be used for RMA, expansion within a node, and expansion of cluster (with new nodes). All methods are all supported, however, they may require upgrading to a specific release which is also identified in the transition release notes.

5.0 Key Management

Q 5.1: What is Key Management?
A 5.1: Key management is the tasks involved with protecting, storing, backing up and organizing encryption keys. HX implements this in a UCSM centric policy.

Q 5.2: What mechanism provides support for key configuration?
A 5.2: UCSM provides support to configure security keys.

Q 5.3: What type of key management is available?
A 5.3: Local management of keys is supported, along with enterprise class remote key management with 3rd party key management servers.

Q 5.4: Who are the remote key management partners?
A 5.4: We currently support Vormetric and Gemalto (Safenet) and includes high availability (HA). Hytrust is in testing.

Q 5.5: How is remote key management implemented?
A 5.5: Remote key management is handled via KMIP 1.1.

Q 5.6: How is local management configured?
A 5.6: The security key (KEK) is configured in HX Connect, directly by the user.

Q 5.7: How is remote management configured?
A 5.7: The remote key management (KMIP) server address information along with login credentials is configured in HX Connect by the user.

Q 5.8: What part of HX communicates with the KMIP server for configuration?

A 5.8: The CIMC on each node uses this information to connect to the KMIP server and retrieve the security key (KEK) from it.

Q 5.9: What types of Certificates are supported in the key generation/retrival/update process?
A 5.9: CA signed and self-signed certificates are both supported.

Q 5.10: What workflows are supported with the encryption process?
A 5.10: Protect/unprotect using a custom password is supported along with local to remote key management conversion. Re-key operations are supported. Secure disk erase operation are also supported.

6.0 User Workflow: Local

Q 6.1: In HX Connect, where so I set up local key management?
A 6.1: In the Encryption dashboard select the configure button and follow the wizard.

Q 6.2: What do I need to have ready to go to get this started?
A 6.2: You will need to provide a 32-character security passphrase.

Q 6.3: What happens if I need to insert a new SED?
A 6.3: In UCSM you will need to edit the local security policy and set the deployed key to the existing node key.

Q 6.4: What happens when I insert the new disk?
A 6.4: If the security key on the disk matches that of the server (node) it automatically gets unlocked. If the security keys are different, the disk will show as a "Locked". You can either clear the disk to delete all data or unlock it by providing the correct key. This is a good time to engage TAC.

7.0 User Workflow: Remote

Q 7.1: What are some things I need to watch out for with remote key management configuration?
A 7.1: Communication between the cluster and the KMIP server(s) happens over the CIMC on each node. This means that the hostname can be used for KMIP server only if the Inband IP address and DNS is configured on the CIMC management

Q 7.2: What happens if I need to replace or insert a new SED?
A 7.2: The cluster will read the identifier from the disk and try to unlock it automatically. If automatic unlock fails, the disk comes up as "locked" and user has to unlock the disk manually. You will have to copy the certificates to KMIP server(s) for credential exchange.

Q 7.3: How do I copy certificates from the cluster to the KMIP server(s)?

A 7.3: There are two ways to do this. You can copy the certificate from the BMC to KMIP server directly or you can use the CSR to get a CA-signed certificate and copy the CA-signed certificate to the BMC using UCSM commands.

Q 7.4: What considerations are there for adding encrypted nodes to a cluster that uses remote key management?
A 7.4: When adding new hosts to the KMIP server(s), the hostname used should be the serial number of the server. To get the KMIP server's certificate, you can use a browser to get the root certificate of the KMIP server(s).

8.0 User Workflow: General

Q 8.1: How do I erase a disk?
A 8.1: In the HX Connect dashboard, select the system information view. From there you can select individual disks for secure erase.

Q 8.2: What if I erased a disk by accident?
A 8.2: When secure erase is used the data is destroyed permanently

Q 8.3: What happens when I want to decommission a node or dissociate a service profile?
A 8.3: None of these actions will remove the encryption on the disk/controller.

Q 8.4: How does encryption get disabled?
A 8.4: The user has to explicitly disable encryption in HX Connect. If the user tries to delete a security policy in UCSM when the associated server has been secured, UCSM will display a config-failure and disallow the action. The security policy has to be disabled first.

9.0 User Workflow: Certificate Management

Q 9.1: How are certificates handled during remote management setup?
A 9.1: Certificates are created using HX Connect and the remote KMIP server(s). Certificates once created will almost never be deleted.

Q 9.2: What kind of certificates can I use?
A 9.2: You can use either self-signed certificates or CA certificates. You have to choose during setup. For CA signed certificates you will generate a set of Certificate Signing Requests (CSRs). The signed certificates are uploaded to the KMIP server(s).

Q 9.3: What hostname should I use when generating the certificates?
A 9.3: The hostname used for generating the certificate should be the Serial Number of the server.

10.0 Firmware Updates

Q 10.1: Are there any restrictions on upgrading the disk firmware?
A 10.1: If an encryption capable drive is detected, any disk firmware changes will not be allowed for that disk.

Q 10.2: Are there any restrictions on upgrading UCSM firmware?
A 10.2: Downgrade of UCSM/CIMC to pre- UCSM 3.1(3x) is restricted if there is a controller which is in secured state.

11.0 Secure Erase Details

Q 11.1: What is Secure Erase?
A 11.1: Secure erase is instant erase of data on the drive (wipe of the disk encryption key). This means that a simple authenticated command can be sent to the drive to change the 256-bit encryption key stored on the drive. This ensures that the drive is wiped clean and there is no data remaining. Even the original host system can't read the data so it will be unreadable by any other system. The operation only takes a couple seconds, as opposed to the many minutes or even hours that it takes to perform an analogous operation on an unencrypted disk and avoids the cost of expensive de-gaussing equipment or services.

Q 11.2: How is secure erase performed?
A 11.2: This is a GUI operation that is performed one drive at a time.

Q 11.3: When is secure erase usually performed?
A 11.3: User initiated secure erase of a single disk is a rare operation. This is mostly done when you want to physically remove the disk for replacement, transfer it to another node, or avoid near future failure.

Q 11.4: What restrictions are there on secure erase?
A 11.4: Secure erase operations can only be performed if the cluster is healthy to ensure that the fault resiliency of the cluster is not impacted.

Q 11.5: What happens if I need to remove an entire node?
A 11.5: There are node remove and node replace workflows to support secure erase of all drives. See the admin guide for details or consult Cisco TAC.

Q 11.6: Can a securely erased disk be reused?
A 11.6: A disk that has been securely erased can be reused in a different cluster only. The secure erase of the SED is done by wiping the disk encryption key (DEK). The data in the disk cannot be decrypted without DEK. This allows you to reuse or decommission the disk without any compromise of the data.

Q 11.7: What happens if the disk I want to erase contains the last primary copy of cluster data?
A 11.7: The data on the disk should have other copies in the cluster to avoid data loss. However, if secure erase is requested on a disk that is the last primary copy, then this operation will be rejected until there is at least one more copy available. Rebalance should be making this copy in the background.

Q 11.8: I really need to securely erase a disk, but the cluster is not healthy. How can I do it?

A 11.8: The command line (STCLI/HXCLI) will allow secure erase when the cluster is not healthy and the disk does not contain the last primary copy, otherwise it is disallowed.

Q 11.9: How can I securely erase an entire node?
A 11.9: This is a rare scenario. Secure erase of all disks in a node is done when one wants to take the node out of the cluster. The intention is either to deploy the node in a different cluster or decommission the node. We can classify node removal in this scenario in two different ways:

1. Secure erase all the disks without disabling encryption
2. Secure erase all the disks followed by disabling encryption for that node (and disks).

Please contact Cisco TAC for assistance.

12.0 Secure Expansion of a Cluster

Q 12.1: What kind of node can I expand an encrypted cluster with?
A 12.1: Only SED capable nodes can be added to an HX Cluster with SEDs.

Q 12.2: How is expansion with local key management handled?
A 12.2: Local key expansion is a seamless operation with no outside configuration required.

Q 12.3: How is expansion with remote key management handled?
A 12.3: Remote key expansion requires lockstep with certificates/key management infrastructure:

- Certificates are required to add new node securely
- The Deployment will show a warning with steps to proceed including a link for certificate download
- The user follows steps to upload certificate(s) and then retries the deployment

13.0 Supporting Documents

Micron:

https://www.micron.com/about/blogs/2016/may/selfencrypting-drives-understanding-the-strategy-of-security

https://www.micron.com/~/media/documents/products/technical-marketing-brief/5100_sed_tcg-e_tech_brief.pdf

https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2667.pdf

https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2382.pdf

FIPS

List of crypto algorithms approved for FIPS 140-2:

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf

CDETS:

- Project: CSC.nuova Product: ucs-blade-server Component: ucsm

SED Functional Specification:

- EDCS: 1574090

SED CIMC Specification:

- http://wwwin-eng.cisco.com/Eng/SAVBU/Projects/Rackmount/Freel_Peak/SW_Specs/Remote_Key_Mgmt_sw_design_spec.doc

Mailing Lists:

- ucsm-dev@cisco.com
- ask-hci-tme@cisco.com
- ask-hci-pm@cisco.com