Managing Encryption

- SED Encryption, on page 1
- HyperFlex Software Encryption, on page 10

SED Encryption

Self-Encrypting Drives Overview

Self-Encrypting Drives (SEDs) have special hardware that encrypts incoming data and decrypts outgoing data in real-time. The data on the disk is always stored in encrypted form. A media encryption key controls this encryption and decryption. This key is never stored in the processor or memory.

A security key, also known as Key-Encryption Key or an authentication passphrase, is used to encrypt the media encryption key. To enable SED, you must provide a security key. No key is required to fetch the data, if the disk is not locked.

Cisco HyperFlex Systems enables you to configure security keys locally or remotely. When you configure the key locally, you must remember the key. In case you forget the key, it cannot be retrieved, and the data is lost if the drive power cycles. You can configure the key remotely by using a key management server (also known as KMIP server). This method addresses the issues related to safe-keeping and retrieval of the keys in the local management.

The encryption and decryption for SEDs is done through the hardware. Thus, it does not affect the overall system performance. SEDs reduce the disk retirement and redeployment costs through instantaneous cryptographic erasure. Cryptographic erasure is done by changing the media encryption key. When the media encryption key of a disk is changed, the data on the disk cannot be decrypted, and is immediately rendered unusable.

An SED based cluster can have encryption enabled and disabled at will. You are free to move between the two states whenever you want. For more information, see the HX-Hardening Guide.

Verify if the HyperFlex Cluster Is Encryption Capable

Verify Using the HX Data Platform Plug-in

1. From the HX Data Platform Plug-in, log into vSphere Web Client.

2. Select **Global Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > Cluster_Name > Summary** > .
3. If the HyperFlex cluster has SED drives and is encryption capable, **Data At Rest Encryption-Capable** is listed at the top of the **Summary** tab.

Verify Using the HX Connect User Interface

1. From the HX Connect UI, select **Encryption**.
2. If the HX cluster has SED drives and is encryption capable, **Data At Rest Encryption-Available** is listed on the **Encryption** page.

Configuring Local Encryption Key

Step 1 On the Cisco HyperFlex Connect Navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, click **Configure encryption**.

Step 3 Enter the following Cisco UCS Manager credentials.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username
Password field	<*admin*> password

Click **Next**.

Step 4 To secure the HyperFlex cluster using an encryption key generated and stored locally, select **Local Key**.

Click **Next**.

Step 5 Enter the **`encryption key (passphrase)`** for this cluster.

Note Enter exactly 32 alphanumeric characters.

Step 6 Click **Enable Encryption**.

Modifying Local Encryption Key

Step 1 On the Cisco HyperFlex Connect Navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, click **Re-key**.

Step 3 Enter the following Cisco UCS Manager credentials.

UI Element	Essential Information
UCS Manager host name field	For example, *10.193.211.120*.
User name field	<*admin*> username.
Password field	<*admin*> password.

Click **Next**.

Step 4 Enter the **Existing Encryption Key** and the **New Encryption Key** for the cluster.

Note Enter exactly 32 alphanumeric characters.

Step 5 Click **Re-key**.

Disabling Local Encryption Key

Step 1 On the Cisco HyperFlex Connect Navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, from the **Edit configuration** drop-down menu, choose **Disable encryption**.

Step 3 Enter the following Cisco UCS Manager credentials.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username
Password field	<*admin*> password

Click **Next**.

Step 4 To disable the encryption key on the cluster, enter the **`encryption key`** in use for the cluster.

Step 5 Click **Disable encryption**.

Step 6 To confirm disabling the encryption key on the cluster, in the **Disable encryption?** dialog box, click **Yes, disable encryption**.

Secure Erase an Encrypted Disk

Step 1 On the Cisco HyperFlex Connect Navigation Pane, choose **System Information**.

Step 2 From the **Disks** tab, select the **`disk`** from which you want to securely erase the local key.

Step 3 Click the **Secure erase** button.

Step 4 To securely erase the encrypted disk on the cluster, enter the encryption key in use on the cluster.

Step 5 Click **Secure erase**.

Step 6 In the **Erase this disk?** dialog box, click **Yes, erase this disk** to securely erase the encrypted disk.

Remote Key Management

The generic steps for remote KMIP certificate handling are as follows:

- If you are self-signing, specify local certificate authority in the configuration and get a root certificate.
- If you are using a trusted third-party CA, then specify that in the configuration and use their root certificate.
- Enter the root certificate in the HX encryption field that asks for the cluster key.
- Create an SSL server certificate and generate a Certificate Signing Request (CSR).
- Sign the CSR with whatever root certificate you are using.
- Update the KMIP server settings to use the client certificate.
- With the SSL certs and root CAs available, proceed with the KMIP service configuration specific to the vendor you have chosen.

SafeNet Key Management

For details on managing encryption keys using a SafeNet key management server, see the SafeNet Admin Guide.

Vormetric Key Management

For details on managing encryption keys using a vormetric key management server, see the Vormetric support portal documentation downloads section.

Configuring Remote Encryption Key

Step 1 On the Cisco HyperFlex Connect navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, click **Configure encryption**.

Step 3 Enter the following Cisco UCS Manager credentials.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username
Password field	<*root*> password

Click **Next**.

Step 4 To secure the HyperFlex cluster using a remote security key generated by the key management (KMIP) server, select **Key Management Server**.

You can configure a server with Self-Encrypting Drives in the cluster to use one of the following certificates.

- **Use certificate authority signed certificates**—Generate Certificate Signing Requests (CSRs) signed by an external certificate authority.
- **Use self-signed certificates**—Generate self-signed certificates.

Click **Next**.

Step 5

What to do next

You can generate certificate signing requests or self-signed certificates.

Generating Certificate Signing Requests

Step 1 On the Cisco HyperFlex Connect navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, click **Configure encryption**.

Step 3 Enter the following Cisco UCS Manager credentials.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username
Password field	<*admin*> password

Click **Next**.

Step 4 Select **Key Management Server** > **Use certificate authority signed certificates**.

Click **Next**.

Step 5 To generate the remote encryption key for configuring the key management (KMIP) server, complete the following details.

UI Element	Essential Information
Email address field	<*admin*> email address.
Organization name field	The organization requesting the certificate. Enter up to 32 characters.

UI Element	Essential Information
Organization unit name field	The organizational unit. Enter up to 64 characters.
Locality field	The city or town in which the company requesting the certificate is headquartered. Enter up to 32 characters.
State field	The state or province in which the company requesting the certificate is headquartered. Enter up to 32 characters.
Country field	The country in which the company resides. Enter two alphabetic characters in uppercase.
Valid for (days) field	The validity period of the certificate.

Step 6 To generate Certificate Signing Requests (CSRs) for all the HyperFlex nodes and download them, click **Generate certificates**.

Step 7 Download the certificates to get them signed by a certificate authority. Click **Close**.

What to do next

1. Upload the signed certificates.
2. Configure KMIP server (key management server).

Configuring a Key Management Server Using CSRs (Certificate Signing Requests)

Before you begin

Ensure that you have downloaded the generated CSRs on your local machine, signed it by a certificate authority and uploaded through the Cisco HX Data Platform UI for configuring the KMIP (key management) server.

Step 1 On the Cisco HyperFlex Connect navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, click **Continue configuration**.

Step 3 From the **Continue configuration** drop-down list, select **Manage certificates** to upload the CSRs.

Step 4 Enter the following Cisco UCS Manager credentials.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username
Password field	<*root*> password

Click **Next**.

Step 5 Select **Upload certificate authority signed certificates**. Click **Next**.

Step 6 Upload the CA signed certificate under **Upload new certificate**. Click **Upload**.

Step 7 From the **Continue configuration** drop-down list select **Configure key management server** to configure the KMIP server.

Step 8 Enter Cisco UCS Manager credentials to set up a primary key management server (KMIP) server and optionally a secondary KMIP server.

UI Element	Essential Information
Primary key management server field	Enter the primary Key Management Server IP address.
(Optional) **Secondary key management server** field	If you have a secondary key management server set up for redundancy, enter the details here.
Port number field	Enter the port number you wish to use for the key management servers.
Public key field	Enter the public root certificate of the certificate authority that you generated during KMIP server configuration.

Step 9 Click **Save** to encrypt the cluster with remotely managed keys.

Generating Self-Signed Certificates

Step 1 On the Cisco HyperFlex Connect navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, click **Configure encryption**.

Step 3 Enter the following Cisco UCS Manager credentials.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username

UI Element	Essential Information
Password field	<*root*> password

Click **Next**.

Step 4 Select **Key Management Server** > **Use self-signed certificates**.

Click **Next**.

Step 5 To generate the remote encryption key for configuring the key management (KMIP) server, complete the following details.

UI Element	Essential Information
Email address field	<*admin*> email address.
Organization name field	The organization requesting the certificate. Enter up to 32 characters.
Organization unit name field	The organizational unit. Enter up to 64 characters.
Locality field	The city or town in which the company requesting the certificate is headquartered. Enter up to 32 characters.
State field	The state or province in which the company requesting the certificate is headquartered. Enter up to 32 characters.
Country field	The country in which the company resides. Enter two alphabetic characters in uppercase.
Valid for (days) field	The validity period of the certificate.

Step 6 To generate self-signed certificates for all the HyperFlex nodes and download them, click **Generate certificates**.

Step 7 Upload the signed certificates and configure KMIP server (key management server).

Configuring a key management server using SSCs (Self-Signed Certificates)

Before you begin

Ensure that you have downloaded the generated SSCs on your local machine to configure the KMIP (key management) server.

Step 1 On the Cisco HyperFlex Connect navigation Pane, choose **Encryption**.

Step 2 On the Encryption Page, click **Edit configuration**.

Step 3 From the **Edit configuration** drop-down list, select **Manage certificates**.

Step 4 Enter the following Cisco UCS Manager credentials, to set up a primary key management (KMIP) server and optionally a secondary KMIP server.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username
Password field	<*admin*> password

Click **Next**.

Step 5 Enter the primary and secondary key management (KMIP) server credentials.

UI Element	Essential Information
Primary key management server field	Enter the primary Key Management Server IP address.
(Optional) **Secondary key management server** field	If you have a secondary key management server set up for redundancy, enter the details here.
Port number field	Enter the port number you wish to use for the key management servers.
Public key field	Enter the public root certificate of the certificate authority that you generated during KMIP server configuration.

Step 6 Click **Save** to encrypt the cluster with remotely managed keys.

Restart Encryption

Enter Cisco UCS Manager credentials to restart configuring the key management server or local key, for securely encrypting the HyperFlex cluster.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username

UI Element	Essential Information
Password field	<*admin*> password

HyperFlex Software Encryption

Enabling HyperFlex Software Encryption Workflow

The following table summarizes the enabling HyperFlex Software Encryption workflow:

Step	Description	Reference
1.	Download the HyperFlex Software Encryption package from My Cisco Entitlements (MCE).	My Cisco Entitlements
2.	Log into the management CIP to install the package on all the controller VMs in the cluster.	Run the command `priv install-package`.
3.	Install the encryption package.	See Install HX Software Encryption Package: Clusters with 13+ Nodes, on page 11.
4.	Follow the enable procedure on Intersight.	Intersight HyperFlex Software Encryption
5.	Verify your cluster is encrypted.	Run the command `hxcli encryption info`.

Note If your cluster has VMware EVC enabled, make sure that the EVC baseline supports nodes with Advanced Encryption Standards New Instructions (AES-NI). If your current EVC baseline does not support AES-NI, change the EVC settings before enabling Software Encryption.

HyperFlex Software Encryption Guidelines and Limitations

Review these guidelines before enabling HyperFlex Software Encryption:

- HyperFlex Software Encryption can be enabled when all HyperFlex Cluster Nodes are running HXDP Release 5.0(1b) and later.
- Support for HyperFlex Stretch Clusters with HyperFlex Software Encryption was introduced in HXDP Release 5.0(2a).
- SED HyperFlex configurations are not supported with HyperFlex Software Encryption.
- HyperFlex Software Encryption is supported only with Vmware ESXi HyperFlex configurations.

- AES-NI enablement is required to install HyperFlex Software Encryption packages on the HX Cluster.
- HyperFlex Software Encryption can not be enabled on existing Datastores.
- HyperFlex Software Encryption can only be enabled on newly created Datastores.
- Once HyperFlex Software Encryption is enabled for a cluster/datastore, it cannot be disabled for the cluster or datastore.
- Once HyperFlex Software Encryption is enabled for a cluster, administrators can create either encrypted or non-encrypted datastores.

Install HX Software Encryption Package: Clusters with 1 - 12 Nodes

Before you begin

Download the HyperFlex Software Encryption package from My Cisco Entitlements (MCE), see My Cisco Entitlements.

Note The HyperFlex Software Encryption package is licensed by its own software PID, which is in addition to the HyperFlex Data Platform and Intersight software licenses. For more information, refer to the Cisco HyperFlex Systems Ordering and Licensing Guide.

Step 1 SFTP the encryption package to the HyperFlex cip node (the node holding the cluster management IP). Use the admin account for the **`username/password`** and a file transfer application, such as winscp. This should upload the package to the /tmp or /home/admin directory.

Step 2 To install the package on all available nodes of a cluster, SSH to the cip node and use the **priv install-package --cluster** option.

Example:

```
priv install-package --cluster --path /tmp/storfs-se-core_<latest version>_x86_64.deb
```

Note Make sure that all nodes are up and not in maintenance mode when using the `--cluster` option to install the encryption package.

What to do next

Go to Intersight HyperFlex Software Encryption to enable encryption on your cluster

Install HX Software Encryption Package: Clusters with 13+ Nodes

Before you begin

Download the HyperFlex Software Encryption package from My Cisco Entitlements (MCE), see My Cisco Entitlements.

Note The HyperFlex Software Encryption package is licensed by its own software PID, which is in addition to the HyperFlex Data Platform and Intersight software licenses. For more information, refer to the Cisco HyperFlex Systems Ordering and Licensing Guide.

Step 1 SFTP the encryption package to each HyperFlex node. Use the admin account for the **username/password** and a file transfer application, such as winscp. This should upload the package to the /tmp or /home/admin directory.

Step 2 For clusters with more than 12 nodes, SSH to each node and use the `priv install-package --local` option.

Example:

```
priv install-package --local --path /home/admin/<package-filename>
```

Note Do not shut down the cluster before proceeding to the next step, enabling HyperFlex Software Encryption. If you shut down the cluster and restart it, you will need to re-install the encryption package.

What to do next

Go to Intersight HyperFlex Software Encryption to enable encryption on your cluster.

Backup Encryption Key of HyperFlex Software Encryption

Encryption keys are stored in multiple copies in a distributed fashion in the cluster. To safeguard against catastrophic failures impacting the entire cluster, it is recommended to create an out-of-band backup of the encryption key to protect against data loss.

Note It is recommended to backup DEK after HX Software Encryption is enabled and after every Rekey. A preivously backed-up DEK cannot be restored after you perform a Rekey on your cluster.

To restore encrypted DEK configuration to the cluster when lost or corrupted from a previously saved back-up, contact TAC.

Step 1 Run the `hxcli encryption backup-keys -f <path to file name>` command.

Note Filename path should start with **/home/admin/**.

Step 2 Enter a passphrase after prompted when the command is executed.

After all the password rules are passed the command completes successfully saving the file in encrypted format.

Note The passphrase should be a minimum of 8 characters in length and should contain at least 1 match of small case characters, at least 1 match of upper case characters, at least 1 match of numerical, and at least 1 match of special characters (one of !@#$%^&*()_+{}?).

Secure Disk Erase for HyperFlex Software Encryption

A software-based disk erase utility that provides the option to do a basic (Mode '0') and standard (Mode '1'/Mode '2') sanitization of the disk. The categorizations are primarily based on the areas of the disk that get sanitized, number of overwrite cycles and patterns on the drive as part of data erasure.

Consider the followings before performing the secure erase operation:

- `secure disk erase` is destructive and irreversible and improper use can lead to data loss.
- `secure disk erase` utility by default checks whether the selected disk contains any last copy of data. This check should not be bypassed.
- `secure disk erase` can be a time-consuming operation depending on the mode of sanitization and the size of the drive.
- You can trigger the secure erase operation from admin mode.
- More than one disk can be sanitized in parallel.

Limitations:

- Boot Disk/Housekeeping disks are not allowed to be secure erased.
- Once a disk is secure erased, the disk can not be re-introduced in the same cluster.
- `secure disk erase` is not supported on SED drives.
- When `secure disk erase` is in-progress, you cannot perform erase on the same disk until it is completed.

Step 1 Run the `secure_disk_erase` command and specify the absolute path of the target disk.

Example:

```
-d DISK_PATH, --disk-path DISK_PATH
```

Step 2 Select from different modes of erase:

Example for basic (default) mode erase (i.e. mode '0'):

Example:

```
admin:~$ secure_disk_erase -d /dev/sdh -m 1

 THIS UTILITY WILL IRRECOVERABLY ERASE DATA FROM DRIVE.PROCEED WITH CAUTION.
 All data (including storfs) from the disk /dev/sdh will be destroyed, proceed [Y/N]:y
 Successfully removed the disk from the system: '/dev/sdh'
 Starting erase operation for disk '/dev/sdh'
     SEAGATE   ST1200MM0009      CN03   peripheral_type: disk [0x0]
       << supports protection information>>
       Unit serial number: WFK25FY70000C917H4GQ
       LU name: 5000c500a762ca2b

 Successfully triggered secure erase operation for the disk: '/dev/sdh'
 Please use following command to track the erase progress:
  secure_disk_erase -d /dev/sdh --progress
```

Step 3 Check erase progress using the following command:

Example:

```
admin:~$ secure_disk_erase -d /dev/sdh --progress
 Fetching the secure erase progress:
 Progress indication: 80.15% don
```

Step 4 After the erase process is completed, physically remove the erased drive from the node.