SED Management

Security Policies for Self Encrypting Drives

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 encrypted in the disk and stored in the encrypted form. The encrypted data is always decrypted on the way out of the disk. A media encryption key controls this encryption and decryption. This key is never stored in the processor or memory. Cisco UCS Manager supports SEDs on Cisco UCS C-Series and S-Series servers.

SEDs are locked using a security key. The security key, which is also known as Key-Encryption Key or an authentication passphrase, is used to encrypt the media encryption key. If the disk is not locked, no key is required to fetch the data.

Cisco UCS Central 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. 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 will render all data on the SED unreadable when the encryption key is destroyed.

Security Guidelines and Limitations for SED Management

The following security guidelines and limitations apply to SED management from Cisco UCS Central:

- Storage operations get applied only when the server is powered on, and they do not trigger a server reboot.
- A global service profile (GSP) with a security policy gets pushed to Cisco UCS Manager releases prior to 3.1(3), and the security policies related operations are cleaned up and an unsecured LUN is created.
- A Cisco UCS Manager downgrade fails if a storage controller with **Drive Security Enable** is present in the domain.

- A GSP association fails with a `config-failure` status/message if it is associated with an unsupported server, or a supported server with unsupported firmware.
- A GSP association fails with a `config-failure` status/message if LUN security is set to **Enabled** in the Disk Configuration Policy but if the Security policy is not created in the storage profile.
- A GSP association fails if the Security policy is deleted from the storage profile after the Storage Controller is set to **Drive Security Enable**.

Security Flags for Controller and Disk

Security flags indicate the current security status of the storage controller and disks.

The storage controller and disks have the following security flags:

- **Security Capable—**Indicates that the controller, LUN, or disk is capable of supporting SED management.
- **Security Enable—**Indicates that the security key is programmed on the controller, disk, or LUN, and security is enabled on the device. This flag is set when you configure a security policy and associate it to a server, making the controller and disk secure. This flag is not set on a Cisco HyperFlex device.
- **Secured—**Indicates that the security key is programmed on the disk, and security is enabled on the Cisco HyperFlex device.

The following security flags are exclusive to storage disks:

- **Locked—**Indicates that the disk key does not match the key on the controller. This happens when you move disks across servers that are programmed with different keys. The data on a locked disk is inaccessible and the operating system cannot use the disk. To use this disk, you must either unlock the disk or secure erase the foreign configuration.
- **Foreign Secured—**Indicates that a secure disk is in foreign configuration. This happens when you unlock a locked disk with the right key, but the disk is in a foreign configuration state and the data on it is encrypted. To use this disk, you can either import or clear the foreign configuration.

Security Related Operations

You can create security policies for Self-Encrypting Drives (SEDs) through a Storage Profile in Cisco UCS Central. In addition to creating security policies, you can perform additional operations on the supported servers. The following table lists the remote operations and their descriptions:

Component	Remote Action	Action
Controller	Unlock Disk	Unlocks ForeignSecured and Locked Disks encrypted using a Local Policy.
	Modify Remote Key	Modifies the Key in the KMIP Server and fetches the new Key for Encryption.
	Disable Security	Disables Security on the Controller when no Secured Disks are present on Controller.
	Unlock for Remote	Unlocks ForeignSecured and Locked Disks encrypted using a Remote Policy.
Virtual Disk	Secure Virtual Drive	Secures LUNs comprised only of SEDs when the Controller is Security Enabled.
Physical Disk	Enable Encryption	Used to Secure JBOD Self-Encrypting Drive(SED) when Controller is Security Enabled.
	Secure Erase	Erases disk cryptographically to make it Unsecured and Reusable.
	Secure Erase Foreign Configuration	Erases ForeignSecured and Locked disks cryptographically to make them Unsecured and Unconfigured Good

For more information about SED Management and security policies, see *Cisco UCS Manager Storage Management Guide*.

KMIP Certification Policy

Cisco UCS Central lets you create a **KMIP Certification** policy to enable communication with the KMIP server for remote management of Self-Encrypting Disks (SED). This policy creates a certificate signing request for the server CIMC. The KMIP Certification policy is supported on Cisco UCS Manager release 3.1(3) and later, Cisco S3260M4 with MegaRAID controllers, and Cisco UCS M4 Blade Servers (C220 and C240M4).

You can create a KMIP Certification policy in the domain scope. Any modification of the certificate in this scope does not result in the regeneration of the certificate. If you want to regenerate a certificate, you must create a KMIP Certification Policy in the **Server** tab in Cisco UCS Manager.

After you create a KMIP Client Certification policy, do one of the following:

- Copy the generated certificate to the KMIP Server.
- Use the generated Certificate Signing Request to get a CA-signed certificate from the KMIP Server and navigate to the **Configure KMIP Certificate** in the Server details page to configure the CA-signed certificate.

Creating or Editing a KMIP Certification Policy

KMIP Certification Policy enables using SEDs through key management servers. This policy aims to generate a certificate that is used by CIMC to communicate with KMIP server to get the key. You can create a KMIP Certification policy from the domain scope.

Step 1 In the **Actions** bar, type **KMIP Certification Policy** and press Enter.

Step 2 In the Create **KMIP Certification Policy** dialog box, select the **Domain Group Location** in which you want to create the policy.

Step 3 Enter a **Name** for the **KMIP Certification Policy**, and add an optional **Description**.
The name is case-sensitive.

Step 4 Fill in appropriate details in the following fields:

- **E-Mail Address—**(Optional) The email address associated with the request. This information is optional.
- **Org Name—**The organization requesting the certificate.
- **Organizational Unit—**(Optional) The organization division that holds the certificate. This field is mandatory if you are using SafeNet KMIP server.
- **Locality—**Locality or city where your organization is located.
- **State—**State or province name.
- **Country Code—**Country name in two upper case letters. For example, US.
- **Validity—**Validity period for the certificate, in number of days.

Step 5 Click **Create**.

Step 6 To edit a KMIP Certification policy, click **Edit** on the policy and change the **Description** and the other details.

Configuring a KMIP Certification Policy

Before You Begin

- Configure the domain in a domain group to refer to the KMIP policy.

Step 1 To configure the policy for the domain scope, select **Domain Configuration Settings** > **Policies** > **KMIP Certification Policy**.

Step 2 In **Policies**, select the KMIP Certification Policy from the drop-down, and click **Save**.
The KMIP Certification policy is configured on the server and you can view the details of the key on the **Server Details** page.