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*.

Enabling Security on a Disk

You can configure the drive security settings for the Self Encrypting Disks using the Storage profile settings.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create storage-profile** *profile-name*	Creates the specified storage profile and enters organization storage profile mode.
Step 4	UCSC(policy-mgr) /org/storage-profile* # **create security**	Creates a security policy for the specified storage profile and enters the security policy mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **create drive-security**	Creates a drive security policy for the specified storage profile security and enters the drive security policy mode.
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security* # **create local**	Creates a local security policy for the specified storage profile and enters the local policy mode.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **set security-key***security-key*	Sets the specified security key for the local policy. The security key must have 32 characters.
Step 8	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **commit buffer**	Commits the transaction to the system configuration.

Creating a Local Security Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create storage-profile** *profile-name*	Creates the specified storage profile and enters organization storage profile mode.
Step 4	UCSC(policy-mgr) /org/storage-profile* # **create security**	Creates a security policy for the specified storage profile and enters the security policy mode.
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **create drive-security**	Creates a drive security policy for the specified storage profile security and enters the drive security policy mode.
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security* # **create local**	Creates a local security policy for the specified storage profile and enters the local policy mode.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **set security-key***security-key*	Sets the specified security key for the local policy. The security key must have 32 characters.
Step 8		

	Command or Action	Purpose
Step 9	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **commit buffer**	Commits the transaction to the system configuration.

Example

```
UCSC # connect policy mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr)# create storage-profile stp-demo

UCSC(policy-mgr)/org/storage-profile* # create security
UCSC(policy-mgr)/org/storage-profile/security* # create drive-security
UCSC(policy-mgr)/org/storage-profile/security/drive-security* # create local
UCSC(policy-mgr)/org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCSC(policy-mgr)/org/storage-profile/security/drive-security/local* # commit-buffer
```

Modifying the Security Policy from Local to Remote

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **scope storage-profile** *profile-name*	Enters the specified storage profile configuration mode for the specified storage profile.
Step 4	UCSC(policy-mgr) /org/storage-profile # **scope security**	Enters the security policy mode for the specified storage profile.
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **scope drive-security**	Enters the drive security policy mode for the specified storage profile security.
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security # **create remote**	Creates and enters the remote policy mode.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set deployed-security-key***existing-security-key*	Specifies the existing key deployed on the server.
Step 8	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set primary-server***primary-server-name*	Sets the primary server hostname or IP address.

	Command or Action	Purpose
Step 9	(Optional) UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set secondary-server***secondary-server-name*	(Optional) Sets the secondary server hostname or IP address.
Step 10	(Optional) UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set port***kmip-server-port-number*	Sets the port number of the KMIP server. KMIP server port numbers can range from 1024 to 65535.
Step 11	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set server-certificate**	Sets the KMIP certificate to the remote security policy.
Step 12	(Optional) UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set timeout** *timeout*	Sets the number of seconds in which communication between the storage and the KMIP server times out. Timeout can range from 5 seconds to 20 seconds.
Step 13	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **commit-buffer**	Commits the transaction to the system configuration.
Step 14	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **exit**	Enters the drive security policy mode.

Modifying the Security Key of a Local Security Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **scope storage-profile** *profile-name*	Enters the specified storage profile configuration mode for the specified storage profile.
Step 4	UCSC(policy-mgr) /org/storage-profile # **scope security**	Enters the security policy mode for the specified storage profile.
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **scope drive-security**	Enters the drive security policy mode for the specified storage profile security.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security # **scope local**	Enters the local policy mode for the the specified storage profile.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local*# **set deployed-security-key***existing-security-key*	Specifies the existing key deployed on the server to configure a new key.
Step 8	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local*# **set security-key***new-security-key*	Sets the new security key for the local policy.
Step 9	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local*# **commit-buffer**	Commits the transaction to the system configuration.

Remote Operations

This section describes the options for configuring security related operations on the controller, local disk, or virtual disk. For more information on the permitted operations, see Security Related Operations, on page 2.

Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCSC(resource-mgr)/domain-mgmt# **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 3	UCSC(resource-mgr)/domain-mgmt/ucs-domain# **scope chassis** *name*	Enters the specific chassis.
Step 4	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis# **scope server** *name*	Enters the specific server.
Step 5	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server# **scope raid-controller** *raid-controller-id*	Enters the RAID controller mode.
Step 6	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server# **set admin-state** name	Set an admin state for the RAID controller. See Security Related Operations, on page 2 for a list of the permitted security operations.
Step 7	(Controller) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/ raid-controller # **set admin-state** unlock-disk*name*	Unlock Disk for a Local Security Policy requires a Key as a parameter. The Key must be 32 characters long.
Step 8	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/ raid-controller # **commit buffer**	Commits the transaction to the system configuration.

	Command or Action	Purpose
Step 9	(Controller) (Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller # **set admin-state** unlock-disk	Unlock Disk for a Remote Security Policy does not require a Key as a parameter.
Step 10	(Local-Disk)(Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller/local-disk # **set admin-state** enable-security	Set security for the local disk.
Step 11	(Local-Disk)(Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller/local-disk # **set admin-state** clear *name* • secure-drive - Equivalent to Secure Erase in the Cisco UCS Central GUI. • secure-foreign-config-drive - Equivalent to Secure Erase Foreign Configuration in the Cisco UCS Central GUI.	These choices are available for a local disk:
Step 12	(Virtual-Disk)(Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller/virtual-drive # **set admin-state** secure-drive-group	