



SED Security Policies

- [Security Policies for Self-Encrypting Drives, on page 1](#)
- [Security Flags of the Controller and Disk, on page 2](#)
- [Managing Local Security Policies, on page 2](#)
- [KMIP Client Certificate Policy, on page 7](#)
- [Managing Remote Security Policies, on page 10](#)
- [Securing an Existing Virtual Drive, on page 14](#)
- [Enabling Security on a Disk, on page 15](#)
- [Erasing a Secure Disk, on page 16](#)
- [Disabling Security on a Controller, on page 17](#)
- [Unlocking a Locked Disk , on page 17](#)
- [Erasing a Secure Foreign Configuration Disk, on page 18](#)
- [Displaying the Security Flags of a Controller , on page 19](#)
- [Displaying the Security Flags of a Local Disk , on page 20](#)
- [Displaying the Security Flags of a Virtual Drive , on page 21](#)

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 SED security policies on Cisco UCS C-Series servers and S-Series servers.

SEDs must be locked by providing 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 Manager enables you to configure security keys locally or remotely. When you configure the key locally, you must remember the key. If 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 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. With Cisco UCS Manager Release 3.1(3), SEDs offer disk theft protection for C-Series and S-Series servers. For HX servers, SEDs offer node theft protection.

Security Flags of the 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 or disk is capable of supporting SED management.
- **Security Enable**—Indicates that the security-key is programmed on the controller or disk, 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 an HX device.
- **Secured**—Indicates that the security-key is programmed on the controller or disk, and security is enabled on the HX 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 the foreign configuration or clear the foreign config.

Managing Local Security Policies

Creating a Local Security Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope org	Enters the root organization mode.
Step 2	UCS-A /org # create storage-profile <i>storage-profile-name</i>	Creates a storage profile with the specified name at the organization level and enters the storage-profile configuration mode.
Step 3	UCS-A /org/storage-profile* # create security	Creates a security policy for the specified storage profile and enters the security policy mode.
Step 4	UCS-A /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.

	Command or Action	Purpose
Step 5	UCS-A /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 6	UCS-A /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 7	UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer	Commits the transaction to the system configuration.

Example

This example show how to create a local security policy with a security key:

```
UCS-A# scope org
UCS-A /org # create storage-profile stp-demo
UCS-A /org/storage-profile* # create security
UCS-A /org/storage-profile/security* # create drive-security
UCS-A /org/storage-profile/security/drive-security* # create local
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

Modifying the Security Key of a Local Security Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope org	Enters the root organization mode.
Step 2	UCS-A /org # scope storage-profile storage-profile-name	Enters the storage-profile configuration mode for the specified storage profile.
Step 3	UCS-A /org/storage-profile # scope security	Enters the security policy mode for the specified storage profile.
Step 4	UCS-A /org/storage-profile/security # scope drive-security	Enters the drive security policy mode for the specified storage profile security.
Step 5	UCS-A /org/storage-profile/security/drive-security # scope local	Enters the local policy mode for the the specified storage profile.

	Command or Action	Purpose
Step 6	UCS-A /org/storage-profile/security/drive-security/local # set deployed-security-key <i>existing-security-key</i>	Specifies the existing key deployed on the server to configure a new key.
Step 7	UCS-A /org/storage-profile/security/drive-security/local* # set security-key <i>new-security-key</i>	Sets the new security key for the local policy.
Step 8	UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer	Commits the transaction to the system configuration

Example

This example shows how to modify the security key of a local security policy:

```
UCS-A# scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # scope local
UCS-A /org/storage-profile/security/drive-security/local # set deployed-security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisnewkey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

Modifying the Security Policy from Local to Remote

Before you begin

Ensure that you have created a KMIP client certificate policy.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope org	Enters the root organization mode.
Step 2	UCS-A /org # scope storage-profile <i>storage-profile-name</i>	Enters the storage-profile configuration mode for the selected storage profile.
Step 3	UCS-A /org/storage-profile # scope security	Enters the security policy mode for the specified storage profile.
Step 4	UCS-A /org/storage-profile/security # scope drive-security	Enters the drive security policy mode for the specified storage profile security.

	Command or Action	Purpose
Step 5	UCS-A /org/storage-profile/security/drive-security # create remote	Creates and enters the remote policy mode.
Step 6	UCS-A /org/storage-profile/security/drive-security/remote* # set deployed-security-key <i>existing-security-key</i>	Specifies the existing key deployed on the server.
Step 7	UCS-A /org/storage-profile/security/drive-security/remote* # set primary-server <i>primary-server-name</i>	Sets the primary server hostname or IP address.
Step 8	(Optional) UCS-A /org/storage-profile/security/drive-security/remote* # set secondary-server <i>secondary-server-name</i>	Sets the secondary server hostname or IP address.
Step 9	(Optional) UCS-A /org/storage-profile/security/drive-security/remote* # set port <i>kmip-server-port-number</i>	Sets the port number of the KMIP server. KMIP server port numbers can range from 1024 to 65535.
Step 10	UCS-A /org/storage-profile/security/drive-security/remote* # set server-certificate	Sets the KMIP certificate to the remote security policy.
Step 11	(Optional) UCS-A /org/storage-profile/security/drive-security/remote* # set timeout <i>timeout-seconds</i>	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 12	UCS-A /org/storage-profile/security/drive-security/remote* # commit-buffer	Commits the transaction to the system configuration.
Step 13	UCS-A /org/storage-profile/security/drive-security/remote # exit	Enters the drive security policy mode.
Step 14	UCS-A /org/storage-profile/security/drive-security # delete local	Deletes the existing local security policy.
Step 15	UCS-A /org/storage-profile/security/drive-security* # commit-buffer	Commits the transaction to the system configuration.

Example

This example shows how to modify a security policy from local to remote:

```
UCS-A # scope org
UCS-A /org # scope storage-profile stp-demo
```

Inserting a Secured Disk into a Server with a Local Security Policy

- The security-key on the drive matches that of the server and it automatically gets unlocked.
- The security-key on the disk is different from the security-key on the server. The disk will appear as a locked disk. You can do one of the following on a locked disk:
 - Erase the secure foreign configuration to delete all data on the disk.
 - Unlock the disk by providing the correct key of the disk. After unlocking the disk, the disk will be in the Foreign Secured state. You must immediately import or clear the foreign configuration for these disks.



Note If you unlock another set of disks before importing the foreign configuration for the current set of disks, the current set of disks become locked again and go in to the Locked state.

KMIP Client Certificate Policy

You can configure the key remotely by using a key management server, which is also known as KMIP server. You must create a KMIP client certificate policy before creating a remote policy. The hostname that is used for generating the certificate is the serial number of the KMIP server.

You can create a certificate policy from two separate scopes:

- Global scope—You can initially create a global certificate policy in this scope. Any modification of the certificate in this scope will not result in the regeneration of the certificate.
- Server scope—You can create or modify a certificate policy in this scope. This will result in a regeneration of the certificates. Such a certificate is specific to the server, and, for this server, overrides the global certificate.

After you create a KMIP client certificate 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. Copy this CA-signed certificate to the CIMC.

Creating a Global KMIP Client Certificate Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope security	Enters the security mode.
Step 2	UCS-A /security # create kmip-client-cert-policy	Creates the KMIP certificate policy and enters the KMIP client certificate policy mode.
Step 3	UCS-A /security/kmip-client-cert-policy* # set country <i>country-code</i>	Specifies the country code for the KMIP certificate policy. The country code must contain 2 letters in upper case.
Step 4	UCS-A /security/kmip-client-cert-policy* # set locality <i>locality-code</i>	Specifies the name of the locality or city for the KMIP certificate policy. Enter up to 32 characters for the locality name.
Step 5	UCS-A /security/kmip-client-cert-policy* # set org-name <i>org-name</i>	Specifies the organization name requesting the KMIP certificate policy. Enter up to 32 characters for the organization name.

	Command or Action	Purpose
Step 6	UCS-A /security/kmip-client-cert-policy* # set org-unit-name <i>unit-name</i>	Specifies the organizational unit name requesting the KMIP certificate policy. Enter up to 64 characters for the organizational unit name.
Step 7	UCS-A /security/kmip-client-cert-policy* # set state <i>state-code</i>	Specifies the name of the state, province, or county for the KMIP certificate policy. Enter up to 32 characters for the state name.
Step 8	(Optional) UCS-A /security/kmip-client-cert-policy* # set email <i>email-address</i>	Specifies the email address associated with the request.
Step 9	(Optional) UCS-A /security/kmip-client-cert-policy* # set validity <i>days</i>	Specifies the validity of the certificate in number of days. The validity can range between 365 days and 3650 days.
Step 10	UCS-A /security/kmip-client-cert-policy* # commit-buffer	Commits the transaction to the system configuration.
Step 11	UCS-A /security/kmip-client-cert-policy # show	Displays details of the KMIP certificate policy.

Example

This example shows how to create a KMIP certificate policy.

```
UCS-A# scope security
UCS-A /security # create kmip-client-cert-policy
UCS-A /security/kmip-client-cert-policy* # set country IN
UCS-A /security/kmip-client-cert-policy* # set locality BLR
UCS-A /security/kmip-client-cert-policy* # set org-name XYZ
UCS-A /security/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A /security/kmip-client-cert-policy* # set state KA
UCS-A /security/kmip-client-cert-policy* # commit-buffer
UCS-A /security/kmip-client-cert-policy # show
```

```
KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /security/kmip-client-cert-policy #
```

Creating a KMIP Client Certificate for a Server

You can create a KMIP client certificate policy for a server. This certificate is applicable only to the specific server, and overrides the global KMIP client certificate.

The hostname that used to create the certificate when using this policy is the serial number of the server.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-number</i>	Enters the server configuration mode for the specified server.
Step 2	UCS-A /server # create kmip-client-cert-policy	Creates the KMIP certificate policy and enters the KMIP client certificate policy mode.
Step 3	UCS-A /server/kmip-client-cert-policy* # set country <i>country-code</i>	Specifies the country code for the KMIP certificate policy. The country code must contain 2 letters in upper case.
Step 4	UCS-A /server/kmip-client-cert-policy* # set locality <i>locality-code</i>	Specifies the name of the locality or city for the KMIP certificate policy. Enter up to 32 characters for the locality name.
Step 5	UCS-A /server/kmip-client-cert-policy* # set org-name <i>org-name</i>	Specifies the organization name requesting the KMIP certificate policy. Enter up to 32 characters for the organization name.
Step 6	UCS-A /server/kmip-client-cert-policy* # set org-unit-name <i>unit-name</i>	Specifies the organizational unit name requesting the KMIP certificate policy. Enter up to 64 characters for the organizational unit name.
Step 7	UCS-A /server/kmip-client-cert-policy* # set state <i>state-code</i>	Specifies the name of the state, province, or county for the KMIP certificate policy. Enter up to 32 characters for the state name.
Step 8	(Optional) UCS-A /server/kmip-client-cert-policy* # set email <i>email-address</i>	Specifies the email address associated with the request.
Step 9	(Optional) UCS-A /server/kmip-client-cert-policy* # set validity <i>days</i>	Specifies the validity of the certificate in number of days. The validity can range between 365 days and 3650 days.
Step 10	UCS-A /server/kmip-client-cert-policy* # commit-buffer	Commits the transaction to the system configuration.
Step 11	UCS-A /server/kmip-client-cert-policy # show	Displays details of the KMIP certificate.

Example

This example shows how to create a KMIP certificate on a server.

```
UCS-A# scope server 5
UCS-A /server # create kmip-client-cert-policy
UCS-A /server/kmip-client-cert-policy* # set country IN
UCS-A /server/kmip-client-cert-policy* # set locality BLR
```

```

UCS-A /server/kmip-client-cert-policy* # set org-name XYZ
UCS-A /server/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A /server/kmip-client-cert-policy* # set state KA
UCS-A /server/kmip-client-cert-policy* # commit-buffer
UCS-A /server/kmip-client-cert-policy* # show

```

```

KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /server/kmip-client-cert-policy #

```

Managing Remote Security Policies

Creating a Remote Security Policy

Before you begin

Ensure that you have created a KMIP client certificate policy.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope org	Enters the root organization mode.
Step 2	UCS-A /org # scope storage-profile <i>storage-profile-name</i>	Enters the storage-profile configuration mode for the selected storage profile.
Step 3	UCS-A /org/storage-profile # create security	Creates and enters the security mode.
Step 4	UCS-A /org/storage-profile/security* # create drive-security	Creates and enters the drive-security mode.
Step 5	UCS-A /org/storage-profile/security/drive-security* # create remote	Creates and enters the remote policy mode.
Step 6	UCS-A /org/storage-profile/security/drive-security/remote* # set primary-server <i>primary-server-name</i>	Sets the primary server hostname or IP address.
Step 7	(Optional) UCS-A /org/storage-profile/security/drive-security/remote* # set secondary-server <i>secondary-server-name</i>	Sets the secondary server hostname or IP address.

	Command or Action	Purpose
Step 8	(Optional) UCS-A /org/storage-profile/security/drive-security/remote* # set port <i>kmip-server-port-number</i>	Sets the port number of the KMIP server. KMIP server port numbers can range from 1024 to 65535.
Step 9	UCS-A /org/storage-profile/security/drive-security/remote* # set server-certificate	Sets the KMIP certificate to the remote security policy.
Step 10	(Optional) UCS-A /org/storage-profile/security/drive-security/remote* # set timeout <i>timeout-seconds</i>	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 11	(Optional) UCS-A /org/storage-profile/security/drive-security/remote* # create login	Creates the login details for the KMIP server and enters the login mode.
Step 12	(Optional) UCS-A /org/storage-profile/security/drive-security/remote/login* # set username <i>username</i>	Sets the username to log into the KMIP server.
Step 13	(Optional) UCS-A /org/storage-profile/security/drive-security/remote/login* # set password <i>password</i>	Sets the password to log into the KMIP server.
Step 14	UCS-A /org/storage-profile/security/drive-security/remote/login* # commit-buffer	Commits the transaction to the system configuration.

Example

```
UCS-A # scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # create security
UCS-A /org/storage-profile/security* # create drive-security
UCS-A /org/storage-profile/security/drive-security* # create remote
UCS-A /org/storage-profile/security/drive-security/remote* # set primary-server 10.10.10.1
UCS-A /org/storage-profile/security/drive-security/remote* # set secondary-server 10.10.10.2
UCS-A /org/storage-profile/security/drive-security/remote* # set port 5696
UCS-A /org/storage-profile/security/drive-security/remote* # set server-certificate
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Certificate:
>-----BEGIN CERTIFICATE-----
MIIEEDCCAvigAwIBAgIGALoFZVDsMA0GCSqGSIb3DQEBCwUAMIGQMSowKAYDVQQD
EyFDRyBDQSBTIG9uIHZvcmlldHJpY2RzbS5jaXNjb5j20xFTATBgNVBAsTDFNh
dmJ1U3RvcmlldjEWMGBGA1UEChMNQ21zY28uU3lzdGVtczERMA8GA1UEBxMIU2Fu
IEpvc2UxExARBgNVBAgTCkNhbgG1mb3JuaWEuXzAxBG9VBAMTUNHIENBIEMGB24g
dm9ybWV0cm1jZHNtLmNpc2NvLmNvbTEVMBMGALUECMMU2F2YnVtdG9yZGV2MRYw
FAYDVQQKEw1DaXNjb5jBTExN0ZW1zMREwDwYDVQQHEWhTYW4gSm9zZTETMB>EGA1UE
CBMkQ2FsaWZvcmlldjEWMGBGA1UEBhMCMVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCdHx2UdIV>TQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
Xwj7yzArflrZ2kVwQcm4f6AdLOFUWzbuo+Fxd3rurd>w6BhJXdLj8Piq8094PqCLp
qdUF83SsRVVbCXHxOqdk9jsSQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
LeKFC8DUEm0G1GQACwiJ3s9O4+P2CI/d4P/>EyWwqABf3YJmA1IEQyUnoTwrg6EgY
```

```

ZvcphsmjXnbBzrL+ON7FBcbrTanvjyJxE6tFf5cRPghymfna7Fd3lfVwZCcGIoR+
> EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbj>BsMBIGA1UdEwEB/wQI
MAYBAf8CAQAwDgYDVR0PAQH/>>>>>>>>>BAQDAgEGMB0GA1UdDgQWBBrnYyFiAK2lEDZJNC0Y
VlIqMgiUJdAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDS
MA0GCSqGSIB3DQEBChwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aesAddQUOCy8fhiPoaMFr1Tgs1hdS0p
NJvfxV6QCun2UMRSuxWfG>0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KESvWW
5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
+U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdnl6uprmvWa3VBk3
OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF>
-----END CERTIFICATE-----

UCS-A /org/storage-profile/security/drive-security/remote* # create login
UCS-A /org/storage-profile/security/drive-security/remote/login* # set username user1
UCS-A /org/storage-profile/security/drive-security/remote/login* # set password Password
UCS-A /org/storage-profile/security/drive-security/remote/login* # exit
UCS-A /org/storage-profile/security/drive-security/remote # exit
UCS-A /org/storage-profile/security/drive-security # show detail expand

```

Drive Security:

Remote:

Primary Server Name: 10.10.10.1
 Secondary Server Name: 10.10.10.2
 KMIP Server Port: 5696
 Deployed Security Key:

KMIP Server Certificate: -----BEGIN CERTIFICATE-----

```

MIIEEDCCAvigAwIBAgIGALOfZVDSMA0GCSqGSIB3DQEBChwUAMIGQMSowKAYDVQQD
EyFDRyBDQSBTIG9uIHZvcmlldHJpY2RzbS5jaXNjb3Y5b20xFTATBgNVBAsTDFNh
dmJlU3RvcmlldjEwMBQGA1UEChMNQ2l2Y28uG3lzdGVtczERMA8GA1UEBxMIU2Fu
IEpvc2UxZzARBgNVBAGTCkNhbgG1mb3JuaWEhXzA5bG9uZzA5bG9uZzA5bG9uZzA5
NzE5MzZmMwVoXDTI2MDkwOTE5MzZmMwVowgZAxKjAoBgNVBAMTIUNHIENBIFMgb24g
dm9ybWV0cm1jZHNtLmNpc2NvLmNvbTEVMBMGAlUECMMU2F2YnVtdG9yZGV2MRYw
FAYDVQQKEw1DaXNjb3Y5b20xFTATBgNVBAsTDFNhdmJlU3RvcmlldjEwMBQGA1UE
CBMKQ2FsaWZvcmlldjEwMBQGA1UEBhMCVGVzZGVzZGVzZGVzZGVzZGVzZGVzZGVzZGVz
DwAwggEKAoIBAQDhX2UdIVTQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
Xwj7yzArflrZ2kVwQcm4f6AdLOFUWzbuo+Fxd3rurdw6BhJXdlJ8Piq8094PqCLp
qdUF83SsRVVbCXHxOqdk9jssQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
LeKFC8DUEm0G1GQACwiJ3s904+P2CI/d4P/EyWwqABf3YJmAI1EQYUnoTwrg6EgY
ZvcphsmjXnbBzrL+ON7FBcbrTanvjyJxE6tFf5cRPghymfna7Fd3lfVwZCcGIoR+
EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbj>BsMBIGA1UdEwEB/wQI
MAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBrnYyFiAK2lEDZJNC0Y
VlIqMgiUJdAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDS
MA0GCSqGSIB3DQEBChwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aesAddQUOCy8fhiPoaMFr1Tgs1hdS0p
NJvfxV6QCun2UMRSuxWfG0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KESvWW
5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
+U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdnl6uprmvWa3VBk3
OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF
-----END CERTIFICATE-----

```

Modifying a Remote Security Key

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters the server mode for the specified server.

	Command or Action	Purpose
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # set admin-state modify-remote-key	Modifies the security key of a remote security policy.
Step 4	UCS-A /server/raid-controller # commit-buffer	Commits the transaction to the system configuration.

Example

This example shows how to modify the remote security key on the controller:

```
UCS-A# scope server 3
UCS-A /server # scope raid-controller 1 sas
UCS-A /server/raid-controller # set admin-state modify-remote-key
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

Modifying the Security Policy from Remote to Local

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope org	Enters the root organization mode.
Step 2	UCS-A /org # scope storage-profile <i>storage-profile-name</i>	Enters the storage-profile configuration mode for the specified storage profile.
Step 3	UCS-A /org/storage-profile # scope security	Enters the security policy mode for the specified storage profile.
Step 4	UCS-A /org/storage-profile/security # scope drive-security	Enters the drive security policy mode for the specified storage profile security.
Step 5	UCS-A /org/storage-profile/security/drive-security # delete remote	Deletes the existing remote security policy.
Step 6	UCS-A /org/storage-profile/security/drive-security* # commit-buffer	Commits the transaction to the system configuration.
Step 7	UCS-A /org/storage-profile/security/drive-security # create local	Creates and enters the local policy mode.

	Command or Action	Purpose
Step 8	UCS-A /org/storage-profile/security/drive-security/local* # set security-key security-key	Sets the security key for the local policy.
Step 9	UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer	Commits the transaction to the system configuration
Step 10		

Example

This example shows how to modify a security policy from remote to local:

```
UCS-A# scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # delete remote
UCS-A /org/storage-profile/security/drive-security* # commit-buffer
UCS-A /org/storage-profile/security/drive-security # create local
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

Inserting a Secured Disk into a Server with a Remote Security Policy

When you insert a secured disk into a server with a remote security policy, the storage disk will appear as a locked disk. Do one of the following:

- Unlock the disk manually with the local key if the disk was previously locked using the local key.
- Unlock using the remote KMIP server.

When you move a secured disk from a server with a local security policy to a server with a remote security policy, the disk will come up as locked. Unlock the disk manually with the local key.

Securing an Existing Virtual Drive

Before you begin

- The controller must be secure.
- The virtual drive must be in the **Orphaned** state.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server# scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller# scope virtual-drive <i>virtual-drive-id</i>	Enters the virtual drive mode for the specified orphaned virtual drive.
Step 4	UCS-A /server/raid-controller/virtual-drive# set admin-state secure-drive-group	Secures the existing virtual drive.
Step 5	UCS-A /server/raid-controller/virtual-drive*# commit-buffer	Commits the transaction to the system configuration.

Example

This example shows how to secure an existing virtual drive:

```
UCS-A# scope server 1
UCS-A /server# scope raid-controller 3 sas
UCS-A /server/raid-controller# scope virtual-drive 1000
UCS-A /server/raid-controller/virtual-drive # set admin-state secure-drive-group
UCS-A /server/raid-controller/virtual-drive*# commit-buffer
UCS-A /server/raid-controller/virtual-drive#
```

Enabling Security on a Disk

Before you begin

Ensure that the disk is a JBOD.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # scope local-disk <i>local-disk-id</i>	Enters the local disk configuration mode

	Command or Action	Purpose
Step 4	UCS-A /server/raid-controller/local-disk # set admin-state enable-security	Enables security on a JBOD.
Step 5	UCS-A /server/raid-controller/local-disk* # commit-buffer	Commits the transaction to the system configuration.

Example

The example shows how to enable security on a JBOD:

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state enable-security
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

Erasing a Secure Disk

Before you begin

Ensure that the disk is in the **Unconfigured Good** state.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # scope local-disk <i>local-disk-id</i>	Enters the local disk configuration mode.
Step 4	UCS-A /server/raid-controller/local-disk # set admin-state clear secure-drive	Erases the secured disk and clears the security on the disk.
Step 5	UCS-A /server/raid-controller/local-disk* # commit-buffer	Commits the transaction to the system configuration.

Example

This example shows how to erase a secure disk:


```

UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state clear secure-drive
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #

```

Disabling Security on a Controller

Before you begin

You can disable security only on SAS controllers. To disable security on a controller, you must first disable security on all the secure disks and delete all the secure virtual drives under the controller.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # set admin-state disable-security	Disables security key on the controller.
Step 4	UCS-A /server/raid-controller # commit-buffer	Commits the transaction to the system configuration.

Example

This example shows how to disable security on the controller:

```

UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state disable-security
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #

```

Unlocking a Locked Disk

When the key of an SED does not match the key on the controller, it shows the disk as Locked, Foreign Secure. You must unlock the disks either by providing the security-key for that disk, or by using the remote KMIP server. After unlocking the disk, import or clear the foreign configuration.

After you unlock a locked disk, the security status of the disk will show as Foreign Secure.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id</i> { <i>SAS</i> <i>SAT</i> }	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SEDs only on SAS controllers.
Step 3	UCS-A /server/raid-controller # set admin-state unlock-disk [<i>security-key</i>]	<p>Unlocks the locked disks.</p> <p>If the security-key is set, this key is used to unlock disks that are in the locked state.</p> <p>If the security-key is not set, Cisco UCS Manager tries to unlock the disks by using the KMIP server. Setting the security-key is optional only if remote security is configured on the server.</p>
Step 4	UCS-A /server/raid-controller* # commit-buffer	Commits the transaction to the system configuration.

Example

This example shows how to unlock a locked disk with a local security policy by using a security-key:

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state unlock-disk thisisastring
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

This example shows how to unlock a locked disk with a remote security policy by using the KMIP server:

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state unlock-disk
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

Erasing a Secure Foreign Configuration Disk

You can erase a secure foreign configuration disk when you have a disk in locked state and you want to use the disk without accessing the existing data.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # scope local-disk <i>local-disk-id</i>	Enters the local disk configuration mode.
Step 4	UCS-A /server/raid-controller/local-disk # set admin-state clear secure-foreign-config-drive	Clears the secure foreign configuration drive.
Step 5	UCS-A /server/raid-controller/local-disk* # commit-buffer	Commits the transaction to the system configuration.

Example

This example shows how to clear a foreign configuration disk:

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state clear secure-foreign-config-drive

UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

Displaying the Security Flags of a Controller

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # show detail	Displays details of the RAID controller.

Example

This example shows to how to check if the security flag of controller is enabled:

```

UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # show detail

RAID Controller:
  ID: 3
  Type: SAS
  PCI Addr: 03:00.0
  Vendor: LSI Corp.
  Model: LSI MegaRAID SAS 3108
  Serial: SV55346948
  HW Rev: C0
  Raid Support: RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
  OOB Interface Supported: Yes
  Mode: RAID
  Rebuild Rate: 30
  Controller Status: Optimal
  Config State: Applied
  Pinned Cache Status: Disabled
  Sub OEM ID: 0
  Supported Strip Sizes: 1MB, 64KB, 256KB, 512KB, 128KB
  Default Strip Size: 64KB
  PCI Slot: HBA
  Controller Flags: Drive Security Capable

```

This example shows to how to check if the security flag of controller is enabled on a blade server:

Displaying the Security Flags of a Local Disk

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # scope local-disk <i>local-disk-id</i>	Enters the local disk configuration mode.
Step 4	UCS-A /server/raid-controller/local-disk # show detail	Displays details of the local disk.

Example

This example shows to how to display the security flag of a local disk:

```

UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas

```

```

UCS-A /server/raid-controller #scope local-disk 2
UCS-A /server/raid-controller/local-disk # show detail

Local Disk:
  ID: 4
  Block Size: 512
  Physical Block Size: 4096
  Blocks: 1560545280
  Raw Size: 763097
  Size: 761985
  Technology: SSD
  Operability: Operable
  Oper Qualifier Reason: N/A
  Presence: Equipped
  Connection Protocol: SAS
  Product Variant: default
  Product Name: 800GB Enterprise performance SAS SED SSD (10 FWPD) - MTFDJK800MBS
  PID: UCS-SD800GBEK9
  VID: V01
  Vendor: MICRON
  Model: S650DC-800FIPS
  Vendor Description: Micron
  Serial: ZAZ090VD0000822150Z3
  HW Rev: 0
  Running-Vers: MB13
  Average Seek Time (R/W): N/A
  Track to Track Seek Time (R/W): 115ms
  Part Number: 16-100911-01
  SKU: UCS-SD800GBEK9
  Drive State: Online
  Power State: Active
  Link Speed: 12 Gbps
  Enclosure Association Type: Direct Attached
  Device Version: MB13
  Drive Security Flags: Secured,Security Enabled,Security Capable

```

Displaying the Security Flags of a Virtual Drive

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope server <i>server-id</i>	Enters the server mode for the specified server.
Step 2	UCS-A /server # scope raid-controller <i>raid-controller-id {SAS SAT}</i>	Enters the RAID controller mode. Currently, Cisco UCS Manager supports SED only on SAS controllers.
Step 3	UCS-A /server/raid-controller # scope virtual-drive <i>virtual-drive-id</i>	Enters the virtual drive mode.
Step 4	UCS-A /server/raid-controller/virtual-drive # show detail	Displays details of the virtual drive.

Example

This example shows how to display the security flag of a virtual disk:

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope virtual-drive 1000
UCS-A /server/raid-controller/virtual-drive # show detail

Virtual Drive:
  ID: 1000
  Name: luna
  Block Size: 512
  Blocks: 20971520
  Size: 10240
  Operability: Operable
  Presence: Equipped
  Lifecycle: Allocated
  Drive State: Optimal
  Type: RAID 0 Striped
  Strip Size (KB): 64
  Access Policy: Read Write
  Read Policy: Normal
  Configured Write Cache Policy: Write Through
  Actual Write Cache Policy: Write Through
  IO Policy: Direct
  Drive Cache: No Change
  Bootable: False
  Oper Device ID: 0
  Change Qualifier: No Change
  Config State: Applied
  Deploy Action: No Action
  Service Profile Lun Reference: org-root/ls-spl/vdrive-ref-lun-1
  Assigned To Server: sys/rack-unit-1
  Available Size on Disk Group (MB): 751745
  Unique Identifier: 90ae6ea0-6a39-49e1-9c0d-0f3e2e9ecfce
  Vendor Unique Identifier: 678da6e7-15b2-9c20-2011-c4f60c40e57a
  Security Flags: Drive Security Enable,Drive Security Capable
```