



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 3](#)
- [KMIP Client Certificate Policy, on page 4](#)
- [Managing Remote Security Policies, on page 6](#)
- [Enabling and Disabling Security on Disks, on page 8](#)
- [Disabling Security on a Controller, on page 9](#)
- [Unlocking a Locked Disk, on page 9](#)
- [Erasing a Secure Foreign Configuration Disk, on page 10](#)
- [Secure Data Deletion, on page 10](#)

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, B-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. Cisco UCS Manager Release 4.0(2) extends the SED security policies to UCS B-Series M5 servers.

Guidelines

To ensure secure and efficient management of Self-Encrypting Drives (SEDs) in Cisco UCS Manager, remember these guidelines:

- The deletion of secured Logical Unit Numbers (LUNs) is only possible using a scrub policy.
- Reconfiguration and deletion of secured LUNs are not allowed on a disassociated server.
- Data sanitization is not permitted until security is enabled.
- If incorrect credentials are provided, the Finite State Machine (FSM) completes without any error, but the LUNs become inoperable, and the drives get locked.
- A power cycle of the server is triggered if any changes are made to the security settings in the storage profile due to the Enterprise Key Management System (EKMS).
- When secured drives are moved between setups, the first association should occur only with security details and no LUN configuration to unlock the drives.
- Changes to login details do not trigger a change. A fresh storage profile association or modification along with other properties, is required.

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

Before you begin

You can create a local policy on a new or existing storage profile.

Procedure

-
- Step 1** In the **Navigation** pane, click **Storage > Storage Profiles**.
 - Step 2** Choose the storage profile where you want to create the policy.
 - Step 3** Click the **Security Policy** tab and then click **Create Security Policy** or right-click the storage profile and select **Create Security Policy**.
 - Step 4** Click the **Local Policy** option.
 - a) Enter **Key**.
The key must consist of 32 alphanumeric characters.
 - b) Click **OK**.
-

What to do next

The key thus created is associated to the storage profile for that server and is deployed under storage controller. To verify this, go to **Server ID > Inventory > Storage > Controller** and select a SAS storage controller. Go to the **General** tab and check whether the **Security** field shows as **drive security enable**.

Modifying a Local Security Policy

Procedure

-
- Step 1** In the **Navigation** pane, click **Storage > Storage Profiles**.
 - Step 2** Choose the storage profile where you have created the policy.
 - Step 3** Click the **Security Policy** tab.
 - Step 4** (Optional) To modify the key for the local policy, in the **Local Policy** area:
 - a) Enter a new security key for the database in the **Key** field.
 - b) Enter the current security key for the database in the **Deployed Key** field.
 - Step 5** (Optional) To change the security policy from **Local Policy** to **Remote Policy**:
 - a) Click the **Remote Policy** option.
 - b) Enter the primary server details in the **IP Address/Hostname** field.

- c) (Optional) Enter the secondary server details in the **IP Address/Hostname** field.
- d) (Optional) Enter the current security key for the database in the **Deployed Key** field.
- e) (Optional) Enter the port number of the server in the **Port** field.
- f) Enter the contents of the KMIP certificate in the **KMIP Server Public Certificate** field.
- g) (Optional) Enter user credentials by clicking **Add Login Details**.

Step 6 Click **Save Changes**.

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

When you insert a secured disk into a server, one of the following will occur:

- 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

You can create a global KMIP client certificate policy.

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** In the **Work** pane, click the **Policies** tab.
- Step 3** Click the **Security** subtab.
- Step 4** Click **Create KMIP Client Cert Policy**.
- Step 5** In the **Create KMIP Client Cert Policy** dialog box that appears, enter the following information:

Name	Description
Country Code	The country code corresponding to the country in which the company resides. Enter two alphabetic characters in upper case.
State	The state or province in which the company requesting the certificate is headquartered. Enter up to 32 characters.
Locality	The city or town in which the company requesting the certificate is headquartered. Enter up to 32 characters.
Organization Name	The organization requesting the certificate. Enter up to 32 characters.
Organization Unit Name	The organizational unit. Enter up to 64 characters.
Email	The email address associated with the request.
Validity	The validity period of the certificate.

- Step 6** Click **OK**.

Creating a KMIP Client Certificate Policy 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

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** For C-Series and S-Series servers, expand **Equipment > Rack-Mounts > Servers > Server ID**.
- Step 3** For B-Series servers, expand **Equipment > Chassis > Chassis ID > Servers > Server ID**.
- Step 4** In the **Work** pane, click the **Inventory** tab and then the **Storage** subtab.
- Step 5** Click the **Security** subtab.
- Step 6** Click **Create KMIP Client Cert Policy**.
- Step 7** In the **Create KMIP Client Cert Policy** dialog box that appears, enter the following information:

Name	Description
Country Code	The country code corresponding to the country in which the company resides. Enter two alphabetic characters in upper case.
State	The state or province in which the company requesting the certificate is headquartered. Enter up to 32 characters.
Locality	The city or town in which the company requesting the certificate is headquartered. Enter up to 32 characters.
Organization Name	The organization requesting the certificate. Enter up to 32 characters.
Organization Unit Name	The organizational unit. Enter up to 64 characters.
Email	The email address associated with the request.
Validity	The validity period of the certificate.

- Step 8** Click **OK**.

Managing Remote Security Policies

Creating a Remote Security Policy

You can create a remote policy on a new or existing storage profile.

Before you begin

Ensure that you have created a KMIP client certificate policy.

Procedure

-
- Step 1** In the **Navigation** pane, click **Storage > Storage Profiles**.
- Step 2** Choose the storage profile where you want to create the policy.
- Step 3** Click the **Security Policy** tab and then click **Create Security Policy** or right-click the storage profile and select **Create Security Policy**.
- Step 4** Click the **Remote Policy** option.
- Enter the primary server details in the **IP Address/Hostname** field.
 - (Optional) Enter the secondary server details in the **IP Address/Hostname** field.
 - (Optional) Enter the port number of the server in the **Port** field.
 - Enter the contents of the KMIP certificate in the **KMIP Server Public Certificate** field.
 - (Optional) Enter user credentials by clicking **Add Login Details**.
 - Click **OK**.
- A message that policy was created successfully is displayed.
-

What to do next

The key thus created is associated to the storage profile for that server and is deployed under storage controller. To verify this, go to **Server ID > Inventory > Storage > Controller** and select a SAS storage controller. Go to **General** tab and check whether the **Security** field shows as **drive security enable**.

Modifying a Remote Security Policy

Procedure

-
- Step 1** In the **Navigation** pane, click **Storage > Storage Profiles**.
- Step 2** Choose the storage profile where you have created the policy.
- Step 3** Click the **Security Policy** tab.
- Step 4** To modify the remote policy, in the **Remote Policy** area:
- Enter the primary server details in the **IP Address/Hostname** field.
 - (Optional) Enter the secondary server details in the **IP Address/Hostname** field.
 - (Optional) Enter the port number of the server in the **Port** field.
 - Enter the contents of the KMIP certificate in the **KMIP Server Public Certificate** field.
Save this certificate from the browser in base-64 format.
 - (Optional) Enter user credentials by clicking **Add Login Details**.
- Step 5** To change the security policy from **Remote Policy** to **Local Policy**:

- a) Click the **Local Policy** option.
- b) Enter a new security key for the controller in the **Key** field.

Step 6 Click **Save Changes**.

Modifying a Remote Security Key

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** For C-Series and S-Series servers, expand **Equipment** > **Rack-Mounts** > **Servers** > **Server ID**.
 - Step 3** For B-Series servers, expand **Equipment** > **Chassis** > **Chassis ID** > **Servers** > **Server ID**.
 - Step 4** In the **Work** area, click the **Inventory** tab.
 - Step 5** Click the **Storage** subtab.
 - Step 6** In the **Controllers** tab, select a SAS controller.
 - Step 7** In the **General** tab, click **Modify Remote Key**.
-

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.

Enabling and Disabling Security on Disks

Before you begin

- To enable security on a disk, ensure that the disk is a JBOD.
- To secure erase a disk, the disk must be in an unconfigured good state.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** For C-Series and S-Series servers, expand **Equipment** > **Rack-Mounts** > **Servers** > **Server ID**.

- Step 3** For B-Series servers, expand **Equipment > Chassis > Chassis ID > Servers > Server ID**
 - Step 4** In the **Work** area, click the **Inventory** tab.
 - Step 5** Click the **Storage** subtab.
 - Step 6** In the **Disks** tab, select a disk.
 - Step 7** In the **Details** area, click **Enable Encryption**.
 - Step 8** To disable a secure disk, click **Secure Erase**.
-

Disabling Security on a Controller

Before you begin

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

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
 - Step 2** For C-Series and S-Series servers, expand **Equipment > Rack-Mounts > Servers > Server ID**.
 - Step 3** For B-Series servers, expand **Equipment > Chassis > Chassis ID > Servers > Server ID**
 - Step 4** In the **Work** area, click the **Inventory** tab.
 - Step 5** Click the **Storage** subtab.
 - Step 6** In the **Controllers** tab, select a SAS controller.
 - Step 7** In the **General** tab, click **Disable Security**.
-

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.

Procedure

- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** Expand **Equipment > Rack-Mounts > Servers > Server Number**.
- Step 3** In the **Work** area, click the **Inventory** tab.
- Step 4** Click the **Storage** subtab.
- Step 5** In the **Controller** tab, select a SAS controller.

- Step 6** To unlock a disk that is secured with a local security policy:
- In the **General** tab, click **Unlock Disk**.
 - In the **Key** text box, provide the key that was used to lock the disk.
 - Click **OK**.
- Step 7** To unlock a disk that is secured with a remote KMIP server, in the **General** tab, click **Unlock For Remote**.

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

What to do next

Import or clear foreign configuration.

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

-
- Step 1** In the **Navigation** pane, click **Equipment**.
- Step 2** For C-Series and S-Series servers, expand **Equipment** > **Rack-Mounts** > **Servers** > **Server ID**.
- Step 3** For B-Series servers, expand **Equipment** > **Chassis** > **Chassis ID** > **Servers** > **Server ID**.
- Step 4** In the **Work** area, click the **Inventory** tab.
- Step 5** Click the **Storage** subtab.
- Step 6** In the **Disks** tab, select a disk.
- Step 7** In the **General** tab, click **Secure Erase Foreign Configuration**.
-

Secure Data Deletion

The Commission Regulation (EU) 2019/424 requires that data be securely disposed of.

Secure data disposal is accomplished by using commonly available tools that erase the data from the various/drives, memory, and storage in the Cisco UCS servers and reset them to factory settings.

Secure data deletion for compliance with Commission Regulation (EU) 2019/424 is supported for the following Cisco UCS servers:

- Cisco UCS B200
- Cisco UCS B480
- Cisco UCS C125
- Cisco UCS C220

- Cisco UCS C240
- Cisco UCS C480
- Cisco UCS S3260

You must be familiar with what devices are present in your UCS server and run the appropriate tools for secure data deletion. In some cases, you may need to run multiple tools.

Full instructions on how to securely erase data are available at: <https://www.cisco.com/web/dofc/18794277.pdf>.

