Key Encryption in Lifecycle Controller

This Dell Technical White Paper provides information about using the Key Encryption in Lifecycle Controller on the 12th Generation servers and later of Dell.

Dell Engineering
December 2013

Balaji K

Bala Gupta

Vinod P S

Sheshadri P.R. Rao

A Dell Technical White Paper

Revisions

Date	Description
Nov 2013	Initial release

Contents

Executive Summary

This whitepaper provides information about using Key Encryption feature in Lifecycle Controller on Dell PowerEdge Servers.

Introduction

Key Encryption is a feature provided in Lifecycle Controller to enable local key encryption, rekey encryption, or delete the encryption key on storage controllers. This feature enables ease of operation by providing an easy-and-simple-to-use interactive GUI. The feature can be used if at least one security-capable controller is present in the system. Otherwise, the link is grayed-out.

Pre-requisits

A system must have any of the following security-capable storage controllers:

- H7XX Series or H7XXp series
- H8XX Series

Local Key Encryption

Local Key Encryption is used to generate an encryption key locally and applies the same on the storage controller.

To create Local Key Encryption:

1. Start Lifecycle Controller. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizard**.
3. Under **Storage Configuration Wizards**, click **Key Encryption**.
4. Select the **Storage Controller** on which you want to create a local key, and then click **Next**.

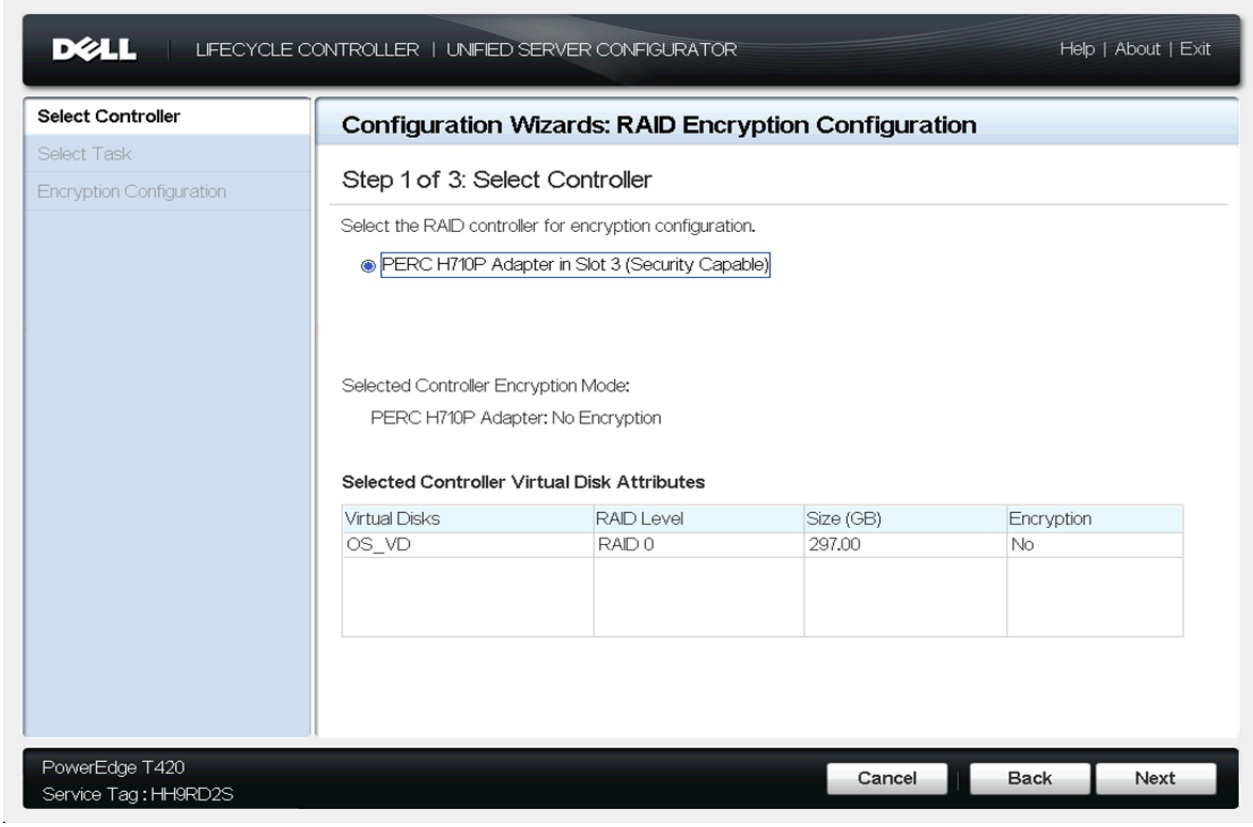

Figure1. Select Storage Controller

5. Click **Setup Local Key Encryption** and click **Next.**

Figure2. Select Encryption Type

6. Type data in the following boxes and click **Finish**.
    a. **Encryption Key Identifier**: Type a unique identifier that is used to identify the encryption key with which the virtual disks are encrypted. This feature enables you to identify the encryption key of the encrypted virtual disks.
    b. **New Passphrase**: Type a security key to encrypt the virtual disks. The controller card uses this passphrase to encrypt the virtual disk data. A valid passphrase must have 8 to 32 characters. A passphrase must include a combination of upper- and lower case letters, numbers, symbols, and must not have white spaces.
    c. **Confirm Passphrase**: Retype the passphrase to confirm. That is, the same security passphrase has to be entered in this field. If an incorrect passphrase is entered, the encryption key is not created, but a warning message is displayed.

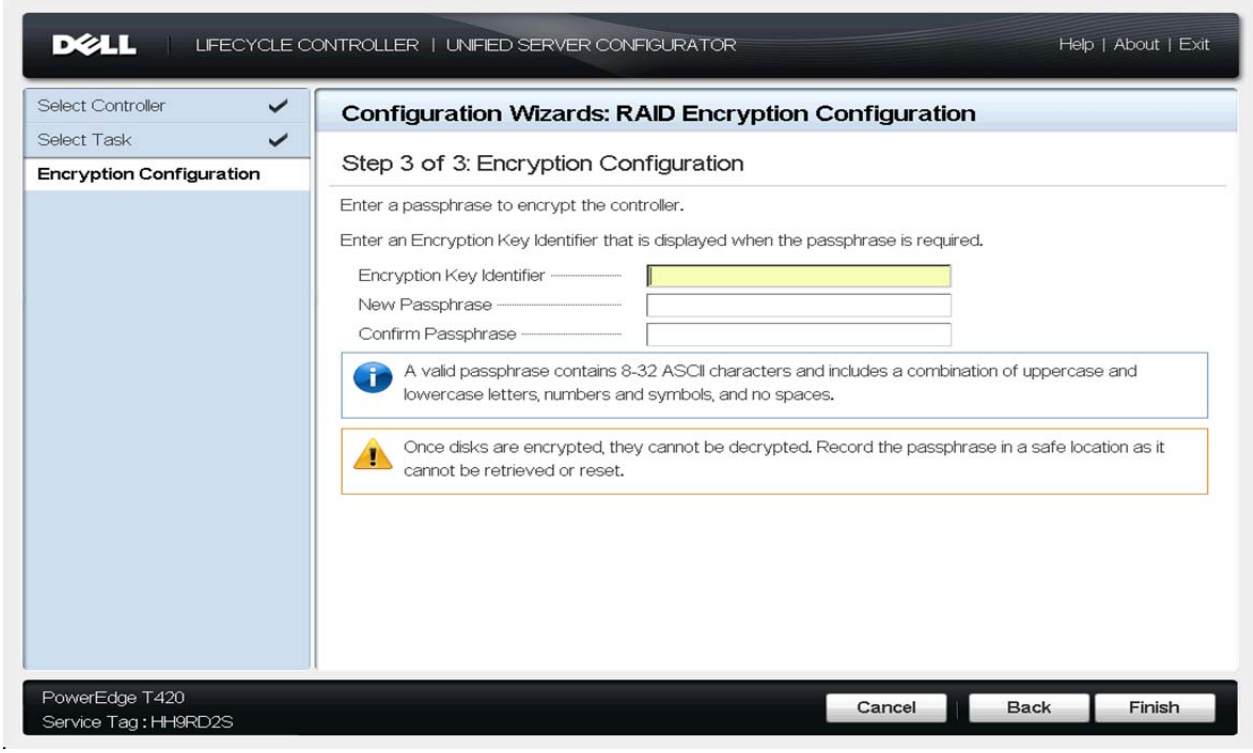

Figure3. Encryption Configuration

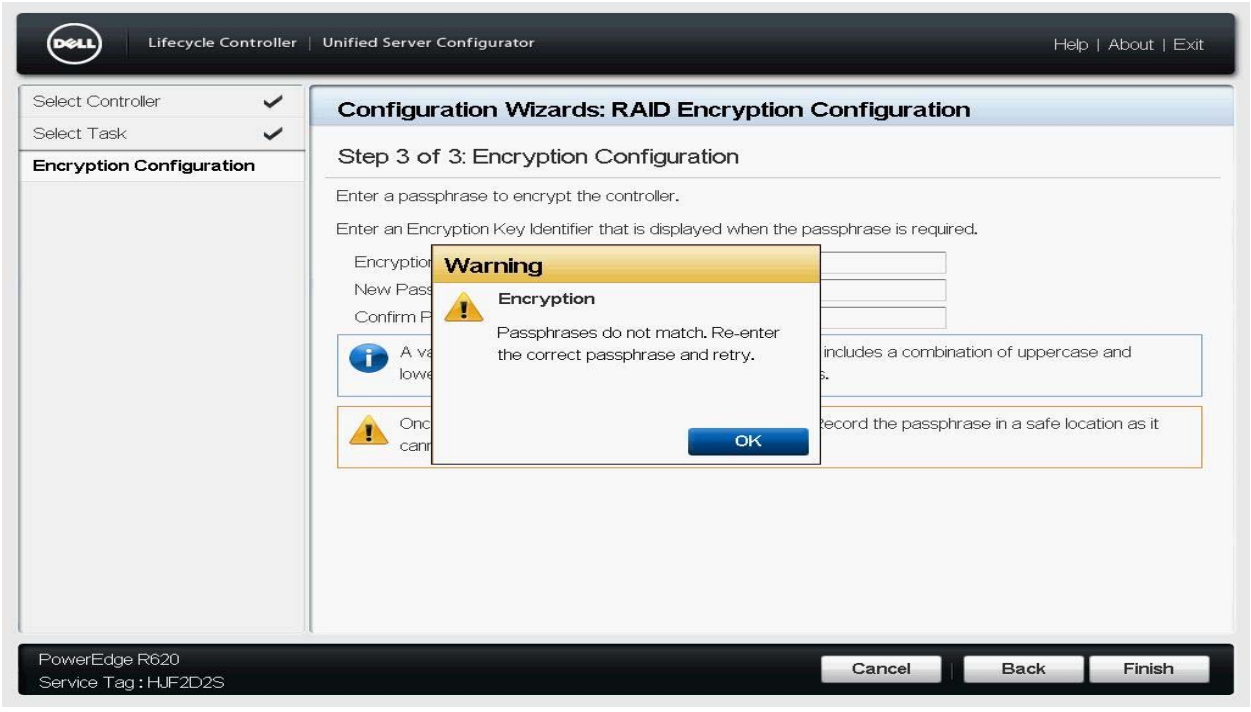

Figure4. Message when passphrase does not match

After you type data in all the boxes, click **Finish**. Lifecycle controller validates the passphrase. If the passphrase fulfills all the criteria, a message is displayed.

Figure5. Security will be enabled on the controller

7. Click **Yes** to create an Encryption key. After successful creation of an ecryption key, a message is displayed.

Figure6. Encryption Key Successfully Created

Encrypting Unsecure Virtual Disks

This feature is used for securing the virtual disks created using RAID Configuration on security-capable disk drives (SEDs—Self Encryption–capable Disks).

To use this option, the pre-requisites are:

- The selected controller must be security-capable
- Self-encryption-capable disk drives with Virtual Disk created on them
- Controller is in local-key-encryption mode

To encrypt an unsecured virtual disk:

1. Start Lifecycle Controller. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizard**.
3. Under **Storage Configuration Wizards**, click **Key Encryption**.
4. Select the **Storage Controller** on which you want to enable this feature and click **Next**.
5. Click the **Encrypt Unsecure Virtual Disk** option, and then click **Next**.

Figure7. Select Encrypt Unsecure Virtual Disks

6. Select a virtual disk you want to encrypt, and then click **Finish**.

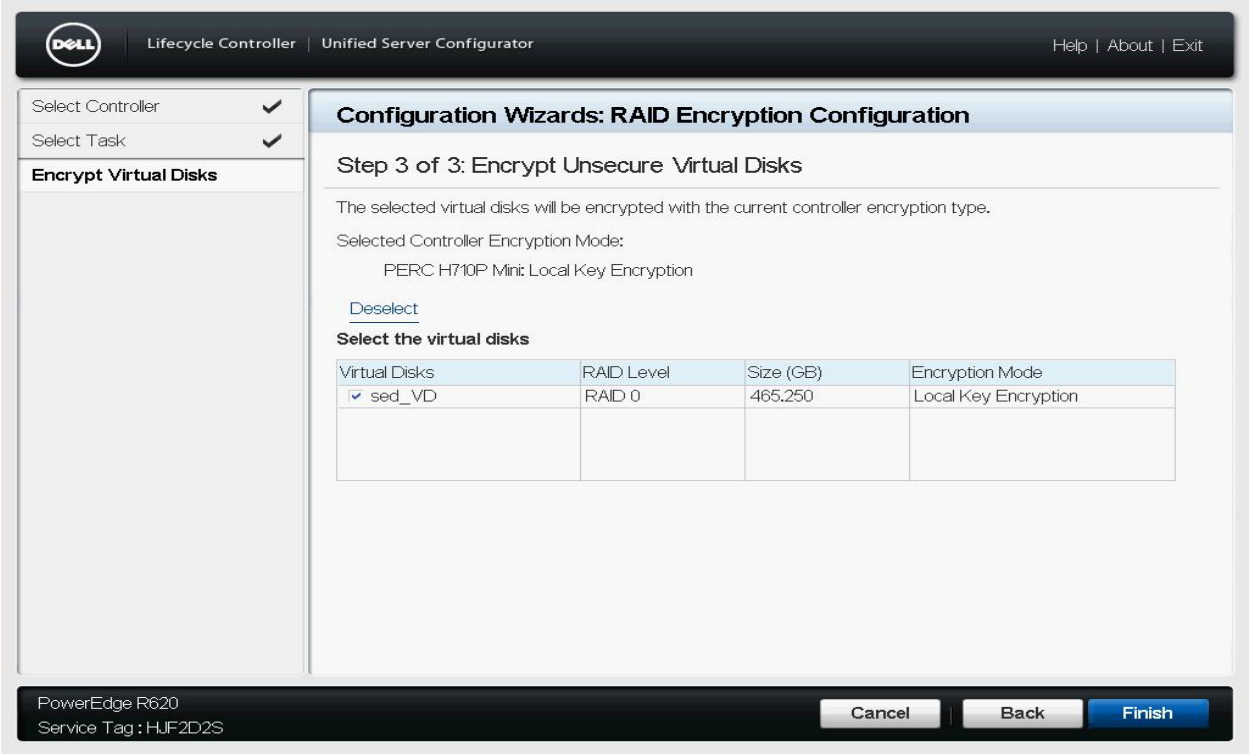

Figure8. Encrypt Unsecure Virtual Disks

Rekeying Controller and Encrypted Disks with a New Local Key

This option is available when the security key is already created on a controller card. You can change the existing security key to another key by using this feature available in Lifecycle Controller.

To rekey the existing security key:

1. Start Lifecycle Controller. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizard**.
3. Under **Storage Configuration Wizards**, click **Key Encryption**.
4. Select the Storage Controller on which you want to enable this feature and click **Next.**
5. Click **Rekey Controller and Encrypted Disks with a New Key**, and then click **Next**.

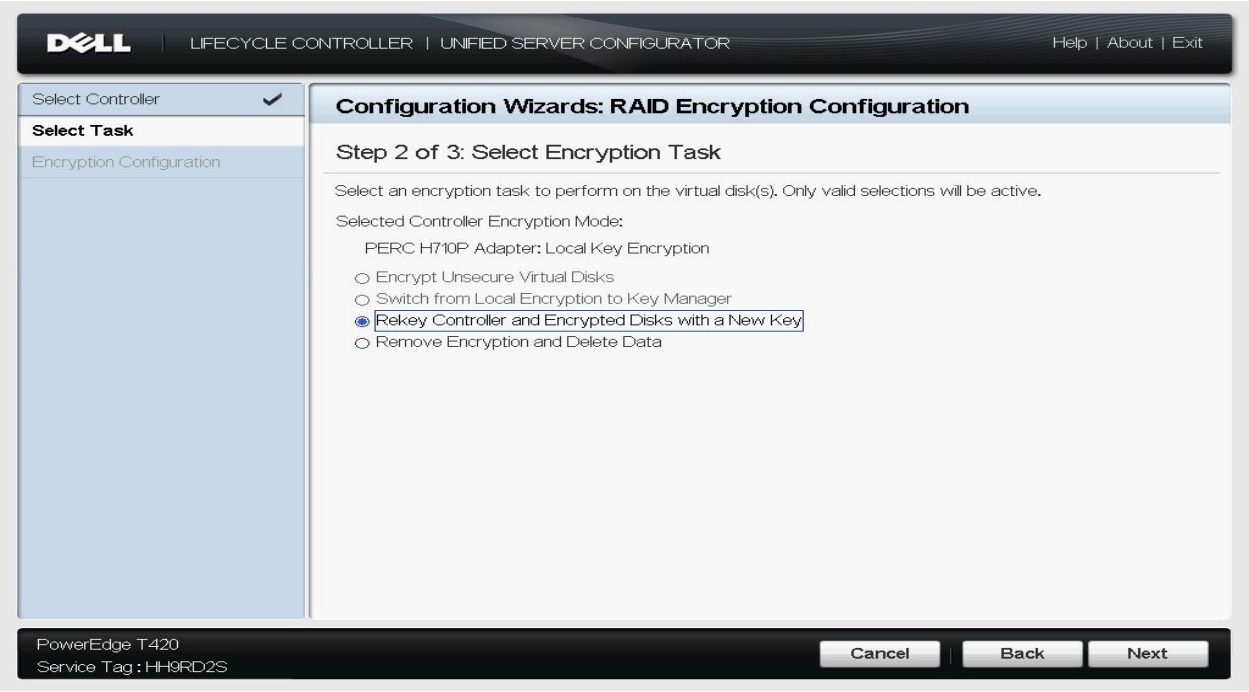

Figure9. Select the Rekey option

6. Type appropriate data in the **Existing Passphrase**, **New Encryption Key Identifier**, **New Passphrase**, and **Confirm Passphrase** text boxes and click **Finish**.

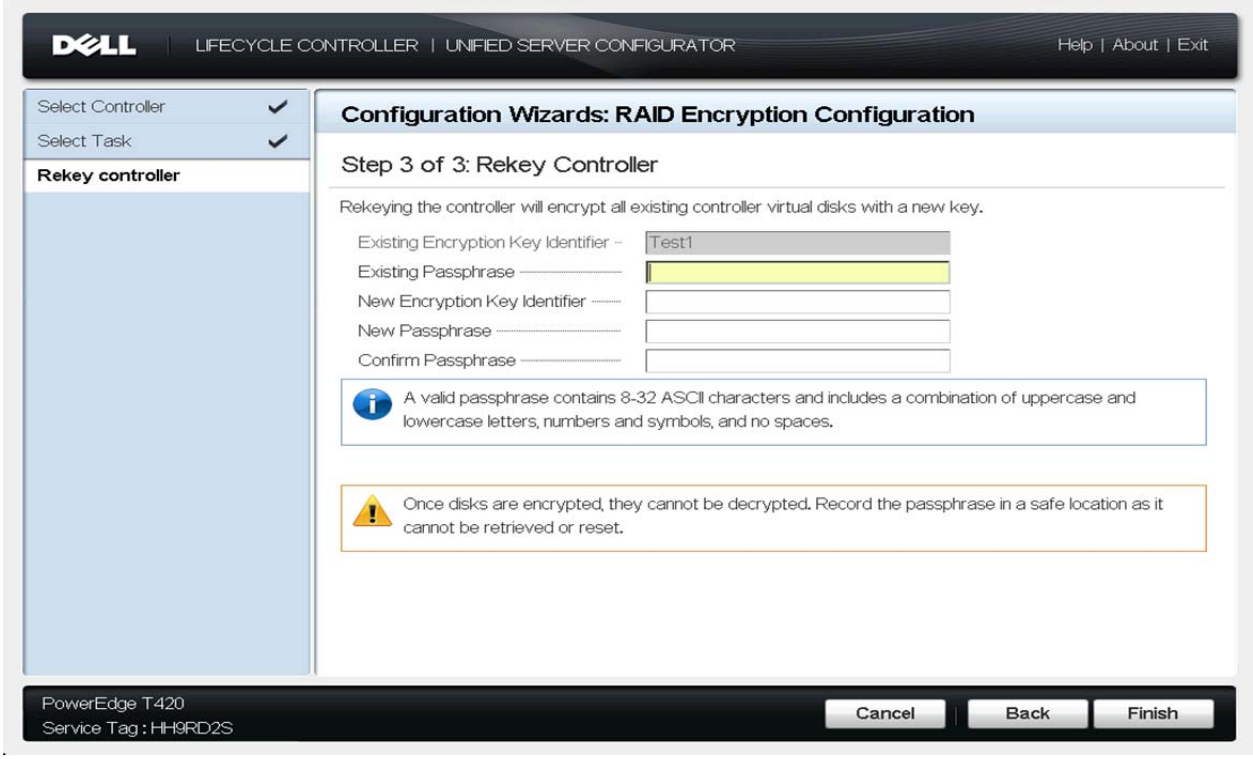

Figure10. Rekey Controller

After clicking **Finish**, Lifecycle Controller validates the existing passphrase, and then the new passphrase. If the validation is successful, a message is displayed.

Figure11. Security will be enabled on the controller

7. Click **Yes** to recreate the key with a new passphrase. After successfully recreating the encryption key, a message is displayed.

Figure12. Key Encryption Successfully Created

Removing Encryption and Deleting Data

This feature is used to disable the encryption already present in the controller and the virtual disks, and then deleting data on the secured virtual disk. To disable the encryption and delete data on the secured virtual disks:

1. Start Lifecycle Controller. In the left pane, click **Hardware Configuration**.
2. In the right pane, click **Configuration Wizard**.
3. Under **Storage Configuration Wizards**, click **Key Encryption**.
4. Select the Storage Controller on which you want to enable this feature and click **Next**.
5. Click the **Remove Encryption and Delete Data** option and click **Next**.

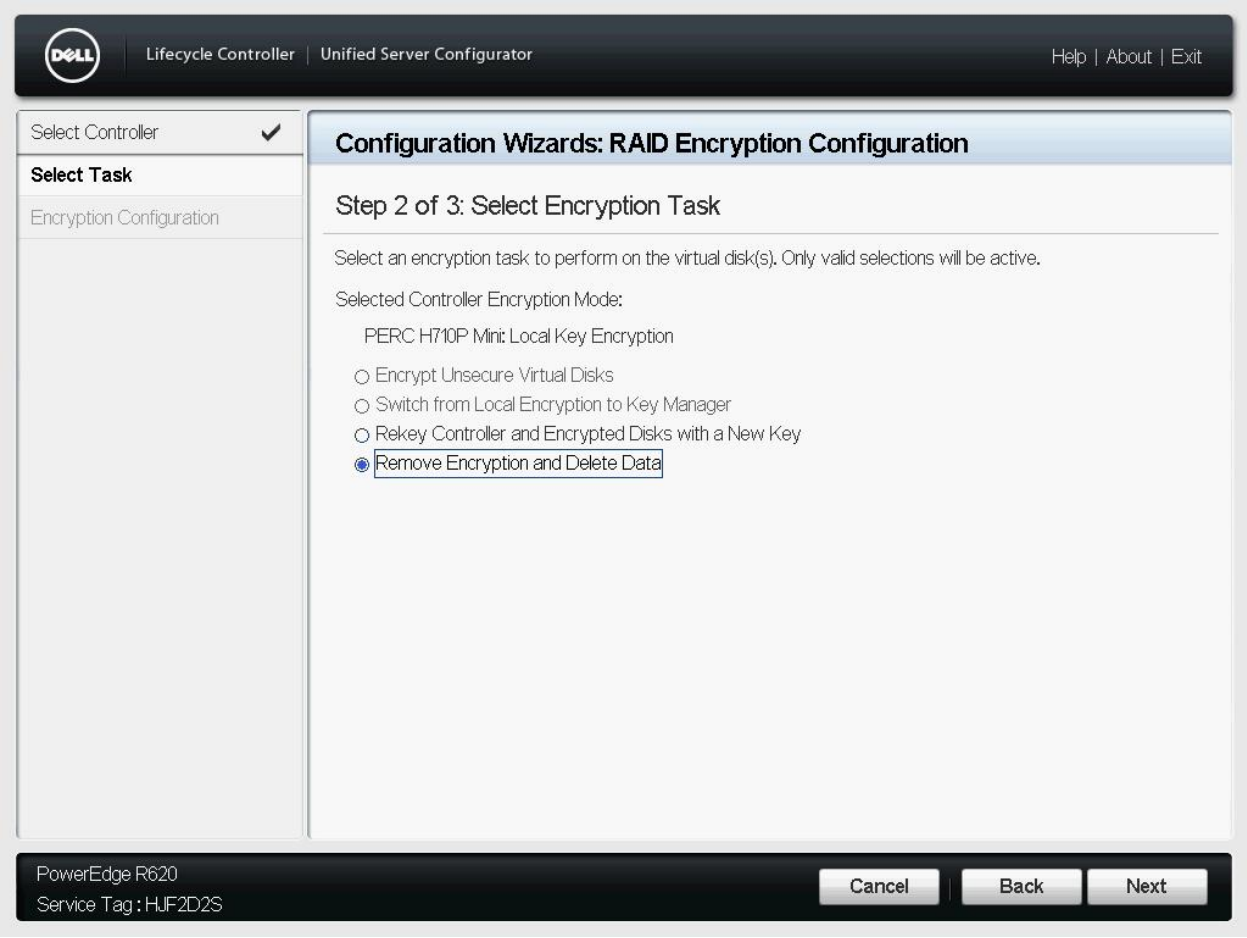

Figure13. Select Encryption Task

6. Select the **Delete encryption key and all the secure virtual disks** option, and then click **Finish**.
   This feature permanently deletes the encryption key, virtual disks, and the data stored on the virtual disks.

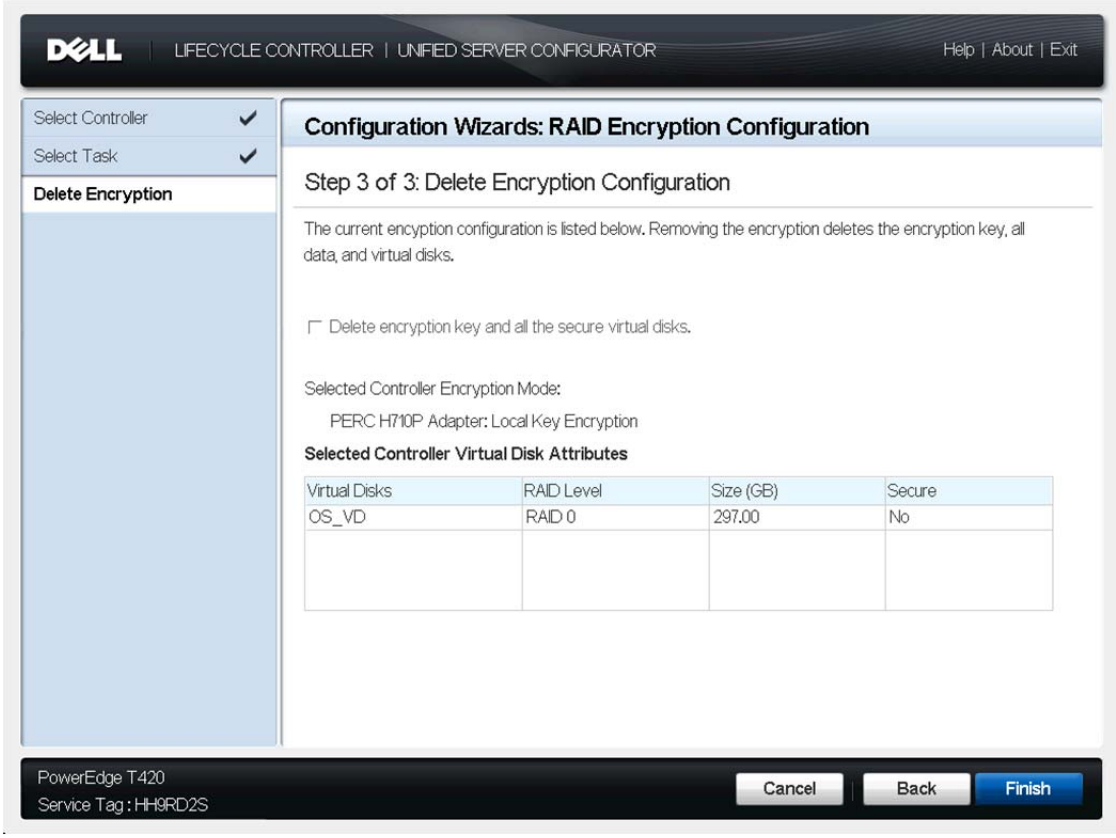

Figure14. Delete Encryption Configuration

After clicking **Finish**, a message is displayed asking whether or not you want to permanently delete data.

Figure15. Delete Encryption Key

7. To delete encryption key and all the secure virtual disks, click **Yes**. After successful deletion of encryption key, a message is displayed.

Figure16. Encryption Key Successfully Deleted