How to Use the Enable Data Encryption Feature on the Cisco Smart Storage

The data encryption feature on the Cisco Smart Storage allows you to encrypt the disk volumes on the NAS with 256-bit AES encryption for data breach protection. The encrypted disk volumes can only be mounted for normal read/write access with the authorized password. The encryption protects the confidential data from unauthorized access even if the hard drives or the entire server were stolen.

.

Contents

About AES Encryption

Advanced Encryption Standard (AES) is a technology standard for encryption. The standard consists of three block ciphers: AES-128, AES-192, and AES-256. Each AES cipher has a 128-bit block size with key sizes of 128, 192, and 256 bits. This is a common encryption standard used worldwide.

Before You Begin

Please beware of the following before you start to use the data encryption feature of the Smart Storage.

- The encryption feature of the Cisco Smart Storage is volume-based. A volume can be a single disk, a JBOD configuration, or a RAID array.
- You have to select whether or not to encrypt your data when you create a disk volume on the NAS. In other words, you will not be able to encrypt a volume after it has been created unless you initialize the disk volume. Note that initializing a disk volume will clear all the existing disk data on it.
- The encryption on the disk volume cannot be removed without initialization. To remove the encryption on the disk volume, you have to initialize the disk volume and all the data will be cleared.
- Please keep the encryption password or key safe. If you forget your password or lose your encryption key, you will not be able to retrieve your data!
- Before you start, please read this document carefully and strictly adhere to the instructions.

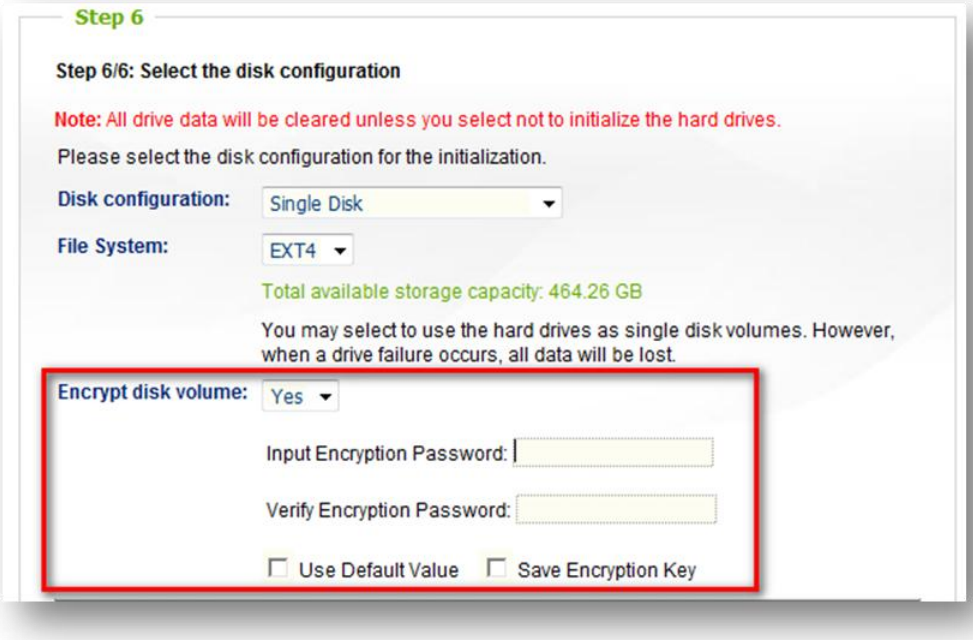
Encrypt Disk Volume During NAS Installation

- Follow the instructions of the Quick Start Guide (QSG) to initialize the NAS by the web-based interface. In the quick configuration steps and when prompted, select **Yes** for the **Encrypt disk volume** option.
    - ❖ Note: You can execute disk volume encryption by the LCD panel if your NAS is equipped with one. Please refer to the QSG for the instructions.

Encrypted Disk Volume

- Once you have selected to encrypt the disk volume, the encryption settings will appear.

Encryption Password



- Enter an encryption password, which will be used to unlock the encrypted volume. The encryption password must be 8-16 characters long and cannot contain spaces ( ). Try to select a long password which combines letters and numbers.
    - Use Default Value: Select to use the default encryption password “admin”.
    - Save Encryption Key: Select to save the encryption key on the NAS (this option can be changed later).
    - If checked: The NAS will unlock the encrypted disk volume automatically using the saved password when it starts up.
    - If not checked: The encrypted disk volume is locked when the NAS starts up. You have to login the NAS as an administrator and enter the encryption password to unlock the disk volume.
- Then proceed to the next step and finish the NAS installation.

Create a New Encrypted Disk Volume with New Hard Drives

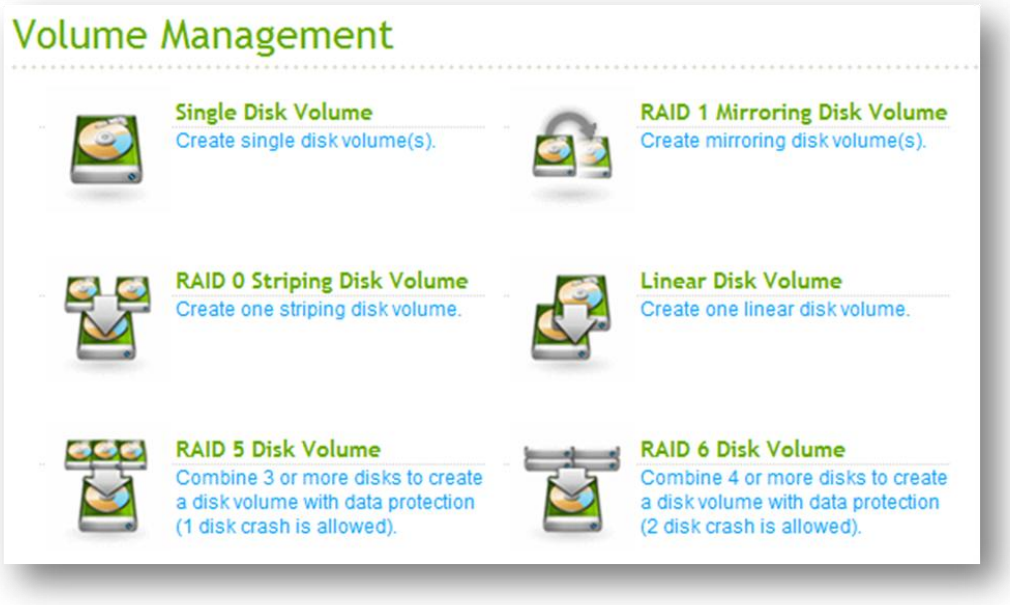
- If your NAS has been installed and you want to create a new encrypted disk volume by installing new hard drives on the server, follow the steps below.

1. Install the new hard drive(s) to the NAS.

2. Login the NAS as an administrator. Choose **Disk Management** > **Volume Management**.

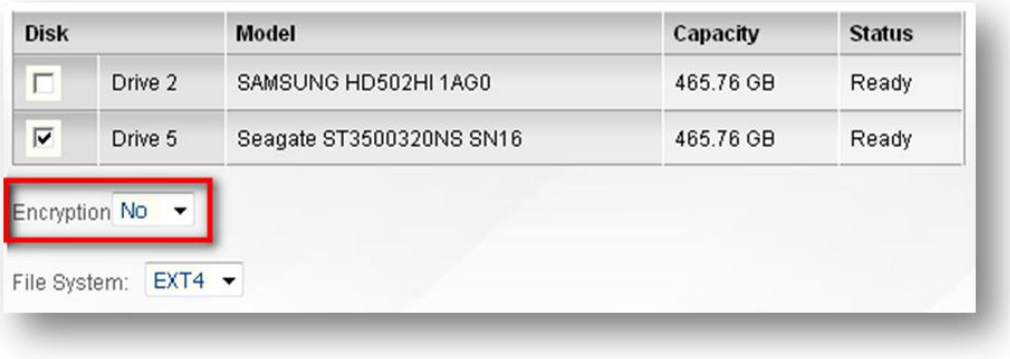
3. Select the disk volume you want to configure according to the number of new hard drives installed.

Volume Management



4. Select the hard drive(s) for creating the disk volume. In this example, we select to create a single drive. The procedure applies also to a RAID configuration.

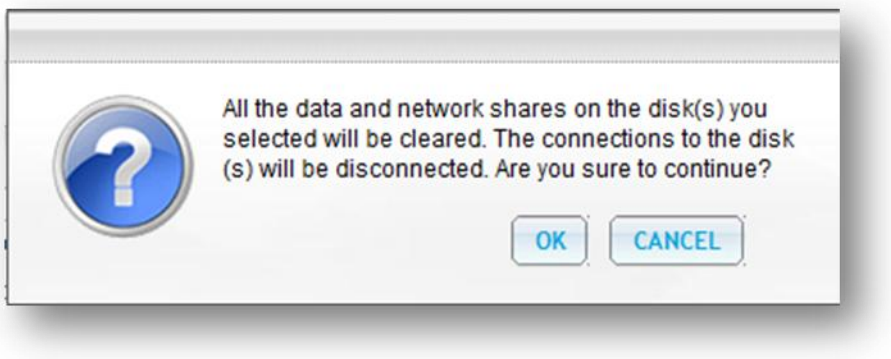
Encryption



5. Select **Yes** for the **Encryption** option and enter the encryption settings.

6. Then click **CREATE** to create the new encrypted volume. Note that all the data on the selected drives will be DELETED! Please back up your data before creating the encrypted volume.

Warning: Data will be cleared

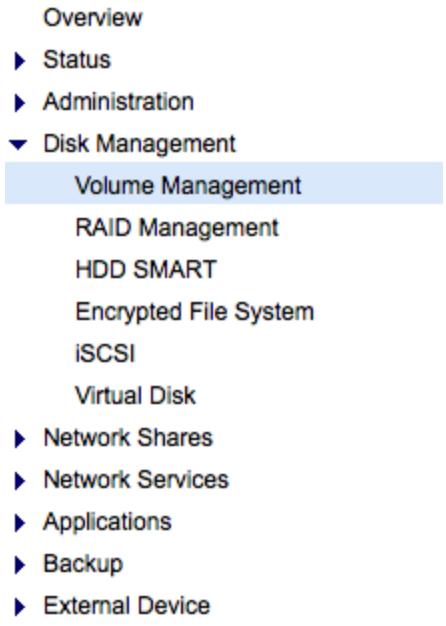


7. You have created a new encrypted disk volume on the NAS.

Verify the Disk Volume is Encrypted

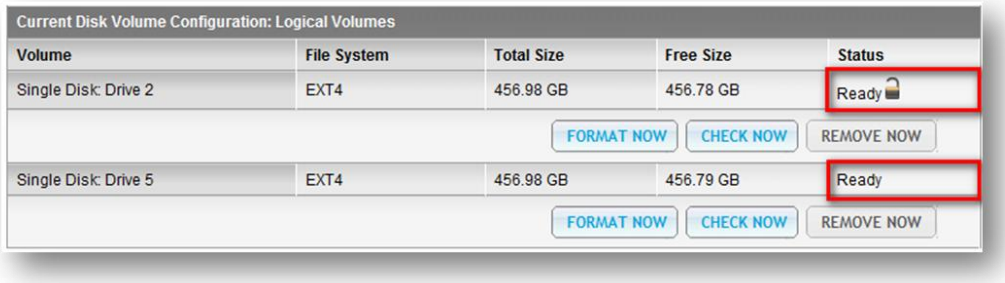
- To verify the disk volume is encrypted, login the NAS as an administrator. Choose **Disk Management** > **Volume Management**.

Volume Management in Menu Tree



- You will be able to see the encrypted disk volume with a lock icon in the Status column.
- The lock will be open if the encrypted volume has been unlocked. A disk volume without the lock icon in the Status column is not encrypted.

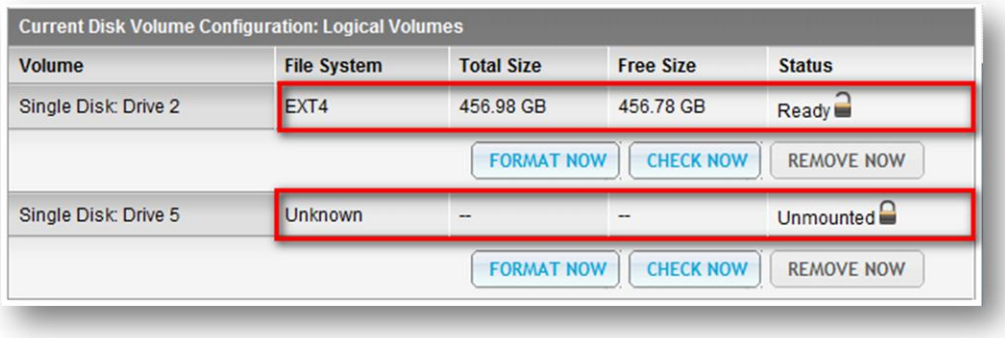
Disk Volume Information



Behavior of Encrypted Volume Upon Reboot

- In this example, we have two encrypted disk volumes on the NAS.
  - ❖ The first volume (Single Disk Drive 2) has been created with the option **Save Encryption Key** enabled.
  - ❖ The second volume (Single Disk Drive 5) has been created with the option **Save Encryption Key** disabled.
- After restarting the NAS, check the volume status. The first drive has been unlocked and mounted but the second drive is locked. Since the encryption key is not saved on the second disk volume, you have to manually enter the encryption password to unlock it.

Disk Volume Status

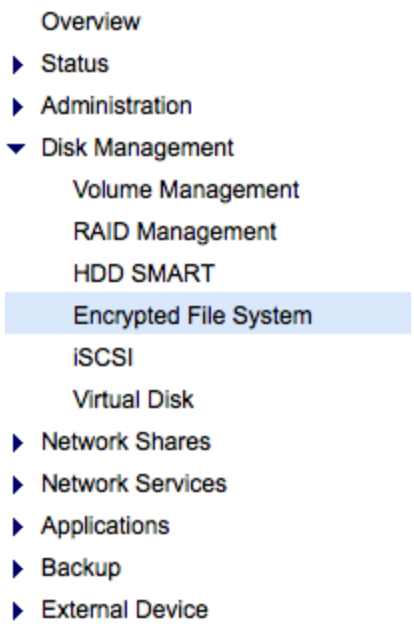


- ❖ Saving the key on the NAS will protect you only if your hard drives are stolen. However, there is a risk of data breach if the entire NAS is stolen as the data is accessible after restarting the NAS.
- ❖ If you select not to save the encryption key on the NAS, your NAS will be protected against data breach even if the entire server is stolen. The disadvantage is that you have to unlock the disk volume manually on each system restart.

Encryption Key Management: New Password, Save Encryption Key, Export

- To manage the encryption key settings, login the NAS as an administrator and choose **Disk Management** > **Encrypted File System**.

Encrypted File System in Menu Tree



- Click **ENCRYPTION KEY MANAGEMENT** on the **Action** column of an unlocked disk volume.

Encryption Key Management

- You can perform the following actions:
  - ❖ Change the encryption key
    - Input your old encryption password and input the new password. (Note that after the password is changed, any previously exported keys will not be working anymore. You have to download the new encryption key if necessary, see below).
  - ❖ Save the encryption key on the NAS
    - Save the encryption key on the NAS for automatic unlocking and mounting the encrypted disk volume when the NAS restarts.
  - ❖ Download the encryption key file

- Input the encryption password to download the encryption key file. Downloading the encryption key file will allow you to save the encryption key in a file. The file is also encrypted and can be used to unlock a volume, without knowing the real password (see **Unlock a Disk Volume Manually** below).
- **Please save the encryption key file in a secure place!**

Encryption Key Management

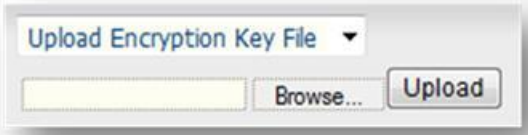
Unlock a Disk Volume Manually

- To unlock a volume, login the NAS as an administrator. Choose **Disk Management** > **Encrypted File System**.
- You will be able to see your encrypted volumes and their status: locked or unlocked.

Encryption Key Management

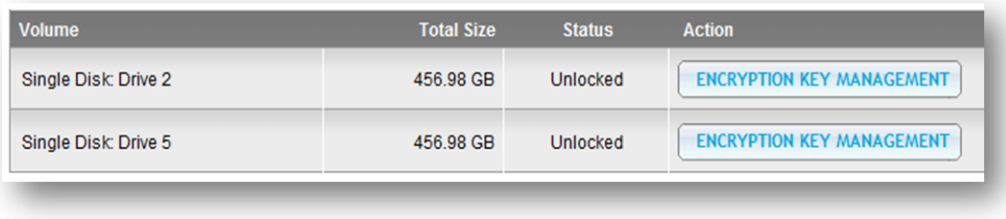
- To unlock your volume, you can either input the encryption password, or use the encryption key file that has been exported previously.

Encryption Key Management



- If the encryption password or the key file is correct, the volume will be unlocked and become available.

Encryption Key Management



For More Information

For more information about Cisco Smart Storage Applications, visit the Cisco Small Business Community forum https://www.myciscocommunity.com/community/smallbizsupport/networkstorage

OL-22122-01