Configure Encryption and Compression

https://campus.barracuda.com/doc/43224760/

Encryption is the process of changing data into a form that cannot be read until it is deciphered, protecting the data from unauthorized access and use. Company policy normally determines when encryption is required. For example, it may be mandatory for company confidential and financial data, but not for personal data. Company policy will also define how encryption keys should be generated and managed.

The current version of Yosemite Server Backup provides the user with the ability to encrypt the data that is written to the media and fully implements the Advanced Encryption Standard (AES) for both hardware and software encryption.

- Hardware encryption is supported on some backup devices, such as HP LTO-4 tape drives. It is faster than software encryption and requires no processing on the backup server. The encryption strength is determined by the backup device. HP LTO-4 tape drives always provide strong AES-256 encryption. This feature can be managed by a backup application that supports hardware encryption, such as Yosemite Server Backup.
- Software encryption uses the encryption algorithms available within Yosemite Server Backup. The user selects an encryption strength: Low 56 bit, Medium 128-bit or High 256-bit. Each encryption key size causes the algorithm to behave slightly differently. Increasing software encryption strength makes the data more secure, but requires more processing power.

If your business requires you to use encryption, Yosemite Server Backup allows you to set the required encryption types and levels. This chapter contains important information about data encryption.

Cryptographic Algorithms

Cryptographic algorithms are the basic components of cryptographic applications. It is important to understand that as you increase the complexity of the encryption the information gets closer to impossible to read and the load on your machine, for software-based encryption, will increase.

Software

Three cryptographic algorithms are provided. These three settings provide three levels of resistance which require progressively more CPU time to convert the same amount of data. The three options are for the software encryption mode only.

- Low – DES 56-bit
- Medium – AES 128-bit

- High – AES 256-bit

Hardware

The cryptographic algorithm provided by hardware devices that provide this feature is not under Yosemite Server Backup control. The hardware provides configuration and operating parameters via a special encryption command. The device driver adjusts its crypto session settings from this input. Hardware encryption is an on/off feature, you do not have the ability to adjust the encryption level through the Yosemite Server Backup interface. By default Yosemite Server Backup will attempt to use the highest encryption algorithm supported on the device, if the device supports multiple algorithms. If the device does not support encryption, the user will be prompted with an alert telling them that the device cannot be used since it does not support hardware encryption.

Passphrase

The passphrase is a series of characters that must be provided by the user for input to the cryptographic key generation process.

- Passphrases must be no less than 8 logical characters. They may be created by the user or randomly generated by a separate application.
- If created by the user, the passphrase should be difficult to guess and should contain a mix of lowercase/uppercase letters, digits and special characters.
- The passphrase is one of the components Yosemite Server Backup uses to generate the encryption key. A longer or random passphrase will increase the strength of the encryption key even more.
- To aid the user in remembering the passphrase, the user may enter a hint message. The use of this field is optional and provided to the user as prompt for remembering the passphrase.
- If a backup job spans multiple media, the same passphrase will be used for all media in the set.

Passphrases for the media are stored in the Yosemite Server Backup catalog. This means the user is able to read and append to the encrypted media without being prompted for a passphrase as long as it is being accessed by the instance of Yosemite Server Backup that first encrypted it.

Once a media is deleted or exported from the Yosemite Server Backup catalog the passphrase is also deleted. There are two instances when the user needs to know the passphrase:

- When importing the media to another machine or another instance of Yosemite Server Backup
- During disaster recovery

Important

Managing the passphrase is a critical component of any encryption system. Data may be stored for months or years, so passphrases must be archived securely. The user should keep a record or backup of encryption passphrases and store them in a secure place separate from the computer running Yosemite Server Backup. If the user is unable to supply the passphrase when requested to do so, neither the user nor Yosemite Server Backup Support will be able to access the encrypted data.

Encryption Options

Encryption is enabled on the job's **Encryption** page.

Option	Description
Off	Both hardware and software encryption are disabled.
Automatic	This selection will use hardware encryption, if it is available from the device; otherwise, software encryption will be used.
Software	Software encryption will be used. When **Software** is selected, the user can choose the strength of software encryption.
Hardware	Hardware encryption will be used, if the device supports it. If it does not support encryption and this option is selected, the user will be prompted with an alert stating that the device cannot be used since it does not support hardware encryption.
Software Strength	Options for the software encryption strength are listed below as three selections, low, medium and high. **Low** is the easiest method to decipher by outside methods, **High** is the hardest method to decipher by outside methods. As you progress from low to high, the encryption algorithm requires more CPU computations for each block of data to be encrypted, which may slow down the data stream to the device and will increase CPU loading on the Media Server.
Encryption passphrase / Verify Passphrase	The user supplied portion of the encryption key. Yosemite Server Backup will use this value, along with other information it generates, to calculate an encryption key for the media. The passphrase must be entered twice to minimize the change of making a mistake while typing.
Hint	The text entered here will be added to the log file of an import job if the media later needs to be imported and the incorrect passphrase is supplied. Use this field to create a reminder of the passphrase as Yosemite Server Backup cannot recover a lost passphrase.

Key Management

Yosemite Server Backup has adopted a very simple key management strategy. A media is encrypted originally by configuring the job that creates it according to the parameters described above. From that point on, the media is known to the catalog. As long as the media is known, restore jobs may use the media without entering the passphrase again. If a media is unknown—because it was deleted from the catalog or because it came from a different catalog—you must import the media to make it known to the catalog again. The import process required you to supply the passphrase to complete the import. If the passphrase supplied does not match that used to encrypt the media, then the hint supplied at encryption time will be shown in the job log so you can try the import again.

When media is encrypted the media is depicted on the **Jobs and Media** view with a lock on it. The Platinum colored lock indicates hardware, whereas the gold lock indicates software encryption. The Media details window shows the type of encryption used.

Compression

Software encryption disables hardware compression, although you will still be able to select **Software compression.**

If the backup device has hardware compression then performance will be better if only hardware compression is used, and that there is little to no benefit of having both enabled. Enabling software compression in this circumstance will reduce performance.

If **Hardware** encryption is selected, we recommend that **Enable hardware compression** is also selected. Hardware encryption and hardware compression can be used on devices, such as the HP LTO-4 tape drive without any loss of backup speed.