

Using External USB Storage Devices with your New Computer

All new Jefferson computers have file-based encryption software called Check Point installed on them. Check Point encryption helps protect your data from unauthorized access.

Checkpoint will also *automatically* encrypt USB external storage devices, such as thumb drives, when they are connected to your computer. This is to help ensure that your Jefferson data remains secure, even when the data is moved or copied to the USB device. Note that Apricorn Aegis USB drives are not encrypted by Check Point since they already contain 256-Bit AES hardware encryption.

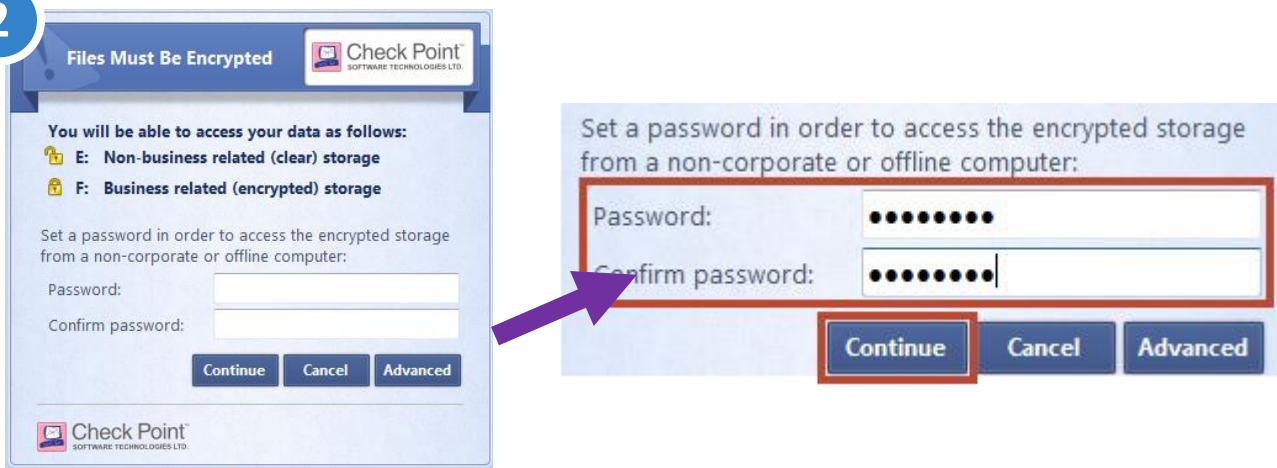
Encrypting Your External Drive

1



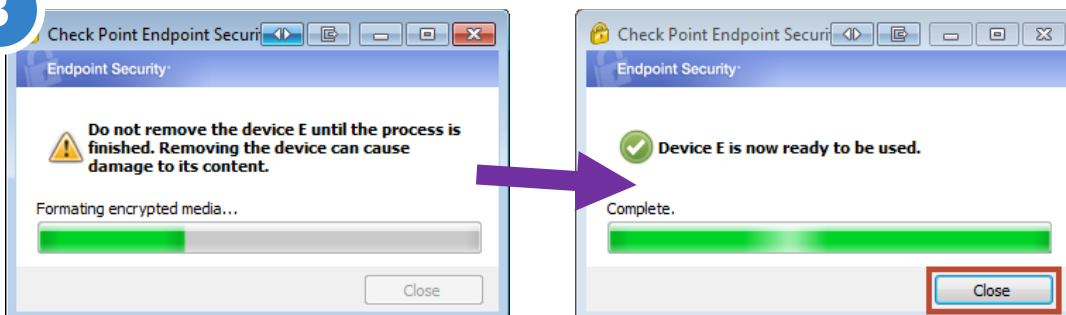
When you connect a USB drive to your computer for the first time, you will be asked to encrypt the drive.

2



Enter and confirm a password. This will be the password that you will use to access the encrypted data on the USB drive. Be sure to choose a secure password that is easy for you to remember. Click **Continue**.

3



Check Point will begin to encrypt your USB drive. When the drive is ready to be used, click **Close**.

Using Your External USB Drive

Once your drive is encrypted, data can be stored in two different partitions:



Business Data - Encrypted

Any *Jefferson* data should be stored here. Data will be encrypted.



Non Business Data

Non-Jefferson data can be stored here. Data will **NOT** be encrypted.

These partitions will show as two different drives on your computer. These drives will behave differently, depending on whether you are using a *Jefferson* computer or a *personal* computer.

Using the USB Drive with a Jefferson Computer

When using the encrypted drive with a *Jefferson* computer running Check Point, you can save and access data on the encrypted USB drive without being prompted for a password.

IS&T recommends that any Jefferson and sensitive data be stored on the Business Data partition of the drive to help ensure that it remains secure if the drive is lost or stolen. Any data stored on the Non Business Data partition can be accessed by anyone who has the USB drive.




Using the USB Drive with a Personal Computer

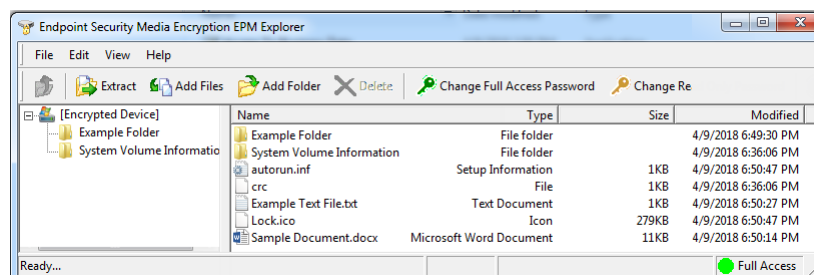


When using the encrypted drive with a *personal* computer, you can save and access data on the *Non Business Data* partition of the drive without being prompted for a password

IS&T recommends that any Jefferson and sensitive data be stored on the *Business Data - Encrypted* partition of the drive to help ensure that it remains secure if the drive is lost or stolen.

To access data stored in the *Business Data – Encrypted* partition:

- 1) Open the  **Access To Business Data** file on your USB drive.
- 2) Enter the password that you created in step 2 above. You now have access to your encrypted data via the *Endpoint Security Media Encryption EPM Explorer*.



If you have any questions or concerns about Check Point encryption, please call the [Solution Center at 215-955-7975](tel:215-955-7975).