Encrypting using FIPS compliant USB devices

A. Introduction

USB flash drives have become common devices in most organizations, thanks to their low cost and ease of use. However, no matter how handy these devices may be, they can also serve as a tremendous source of data leakage. To avoid data leakage caused by USB devices, users are recommended to encrypt data on such removable devices.

BitLocker To Go will be the ideal and ultimate method of performing data encryption for users who has upgraded to Windows 7. Users may refer to our BitLocker To Go User Guide (http://www.cityu.edu.hk/csc/deptweb/support/guidelines/bitLocker_to_go_userguide.pdf) for more information.

For the users who have not yet upgraded to Windows 7, USB devices with built-in security features will be the interim solution for them. Users are recommended to purchase the secure USB devices that are FIPS 140-2 level 2 certified with hardware based 256-bit AES encryption. It is one of the newest government- and corporate-grade encryption standards, and its complexity is more than sufficient to protect your data.

Below are some secure USB devices that are FIPS 140-2 level 2 certified with hardware based 256-bit AES encryption:

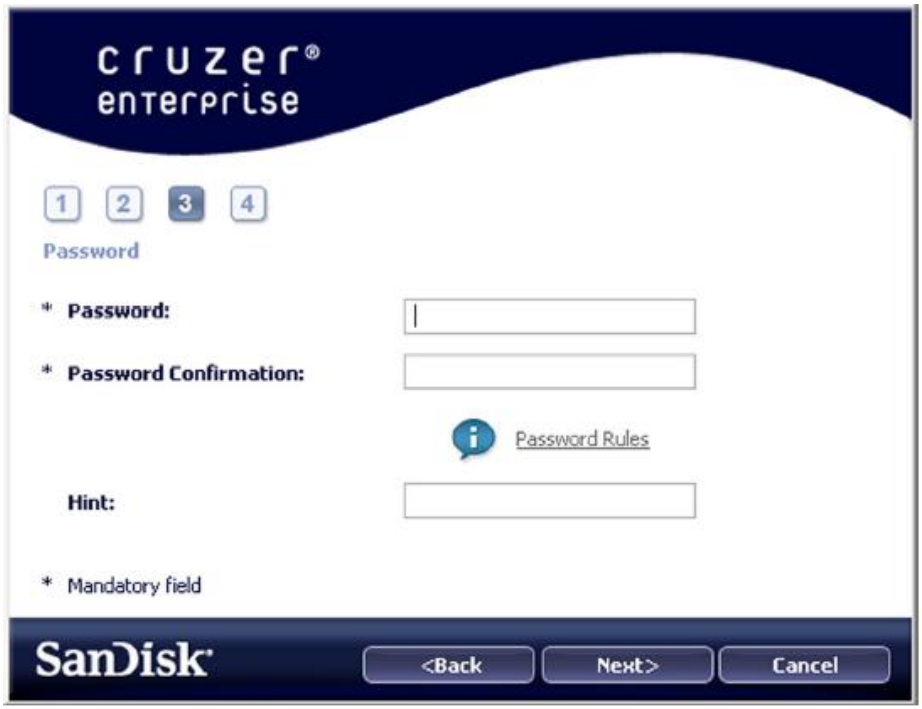
- SanDisk Cruzer Enterprise FIPS Edition
  http://www.sandisk.com/business-solutions/enterprise/cruzer-enterprise-fips-edition
- Kingston DataTraveler BlackBox
  http://www.kingston.com/flash/DTBlackBox.asp
- MXI Stealth MXP Bio
  http://www.mxisecurity.com/categories/display/62

B. Demonstration of Data Protection on SanDisk Cruzer Enterprise FIPS Edition USB Drive

1. Initializing the device

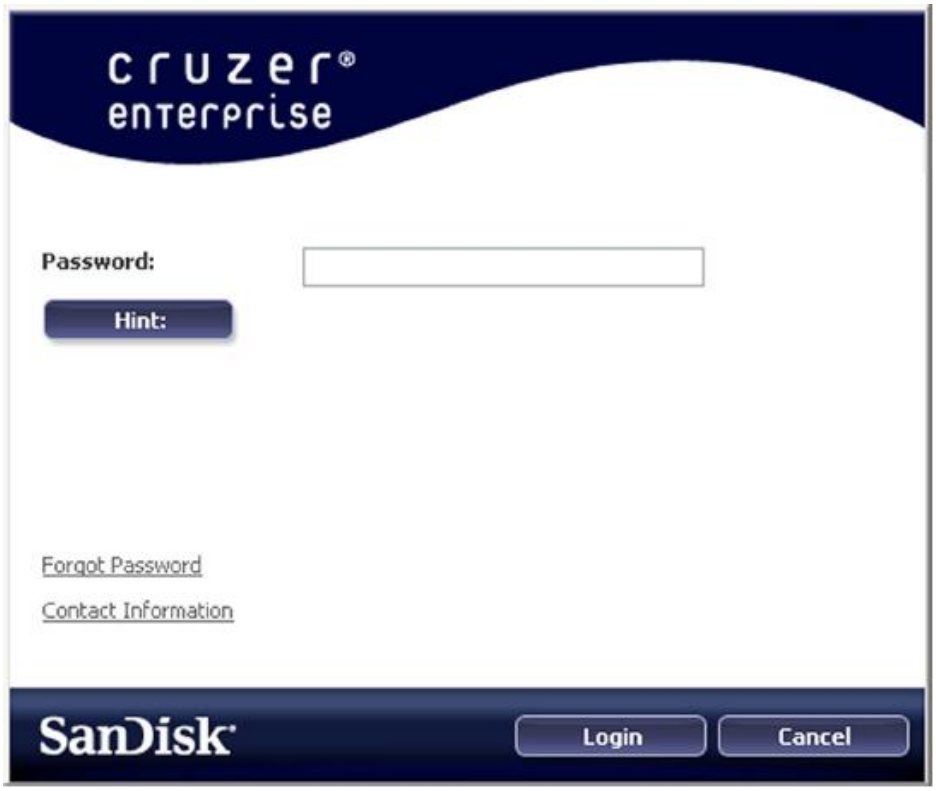
i. Insert the drive into an available USB port

ii. Enter a password and re-enter it for confirmation (strong password should be used. It must contain three different types of characters: lower case letters, upper case letters, numeric digits, or special characters.)
A password hint can be entered to remind you of your password.



iii. A user can optionally type his/her name, company name and details in the Contact Information window. The contact information is displayed on the logon window when clicking the Contact Information link.

2. Using the drive
   i. Insert the drive into an available USB port
   ii. Type your password and click **Login** to access the data on the drive



3. Forgetting your password
   i. The drive includes a “lockdown” mode for enhanced security. This lockdown feature will lock the drive whenever a maximum number of password attempts exceed a pre-configured value. In the event that the device is locked, the device must be reformatted to enable operation. All data on the drive will be erased.
   ii. A lost password will result in the loss of your data. Users can’t access the drive anymore without the password. Therefore, users are recommended to keep the password in a safe place.

C. References

Please refer to the following resources for more information:

1. Advanced Encryption Standard (AES) from Wikipedia
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
2. FIPS PUB 140-2 Security Requirements for Cryptographic Modules from NIST

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf