How to Encrypt USB Sticks and Other Removable Media

Introduction

1. This guideline has been issued by the Chief Information Officer to supplement the Encryption Requirements standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.
2. This document explains how to encrypt USB sticks (flash drives) and other removable devices and media, such as portable drives and CDs to protect the information stored in them from unauthorized access. Alternatively, you can use a hardware-encrypted device, i.e. a device that comes with built-in encryption. A list of hardware-encrypted devices is shown in Appendix A.

Recommended Applications

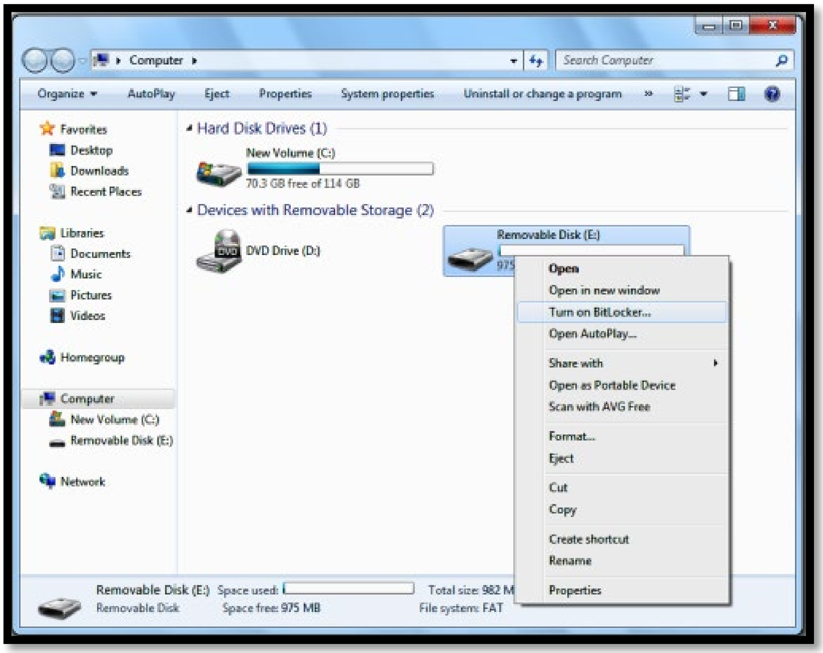
3. This is a list of recommended applications to securely encrypt USB sticks (flash drives) and other removable drives and media:

Product	Purpose	More Information
McAfee Endpoint Encryption	This is the UBC-recommended solution. It is only available if McAfee Endpoint Encryption software has been installed.	http://it.ubc.ca/services/security/encryption-services/mcafee-endpoint-how-encrypt-usb-or-mobile-storage-devices
Microsoft Bitlocker to Go	An alternative solution for Microsoft operating systems	Available with Windows 7 Enterprise and Ultimate Editions and Windows 8 Pro and Enterprise Editions. See below for usage guidance
Apple FileVault 2	An alternative solution for Mac operating systems.	http://support.apple.com/kb/HT4790

How to Encrypt Using BitLocker to Go

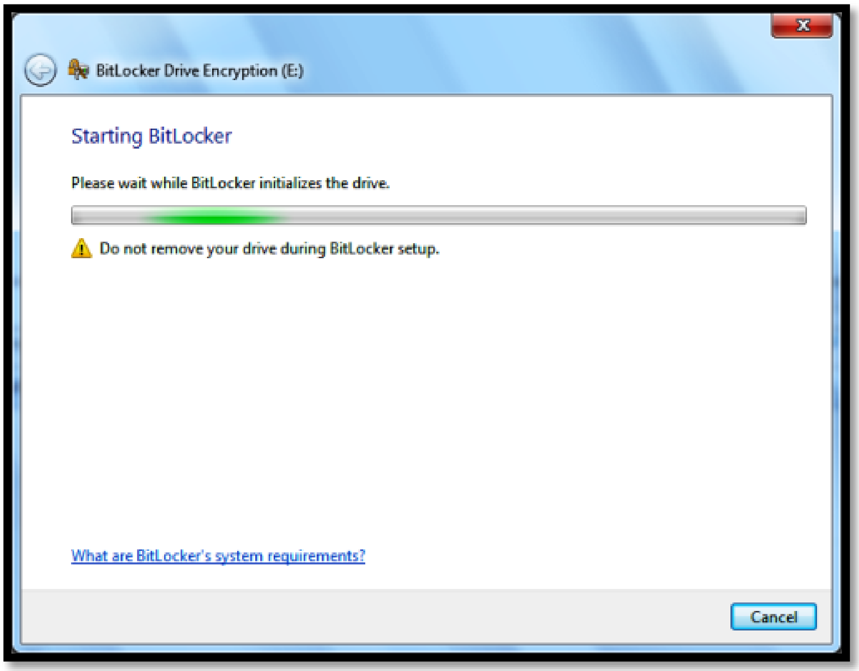
4. If you are using a computer running Windows 7 or 8, BitLocker comes with your system and does not require installation. As long as you have the password, BitLocker To Go encrypted USB Memory sticks can easily be read and edited on these computers.
5. In addition, BitLocker To Go encrypted USB Memory sticks can be read (but not edited) on computers running Windows XP or Vista. The USB Memory stick contains a program called BitLocker To Go Reader. Once it has been installed on the Windows XP or Vista machine, you will be prompted for a password. Once the password is provided and accepted, you will be able to read the files on the USB Memory Stick. However, you will not be allowed to edit, delete or add files to the USB Memory Stick.
6. The instructions below show how to encrypt using Bitlocker to Go:
    a. Open Windows Explorer or My Computer.
    b. Insert your USB Memory Stick in a USB port on the computer.

c. The USB Memory Stick should now be visible to the system. Right click on the drive and select “Turn on BitLocker” from the menu.



Removable Disk (E:) Space used: Total size: 982 M
Removable Disk Space free: 975 MB File system: FAT

d. BitLocker To Go will start initializing the USB Memory Stick. This does not destroy existing data on the Memory Stick.

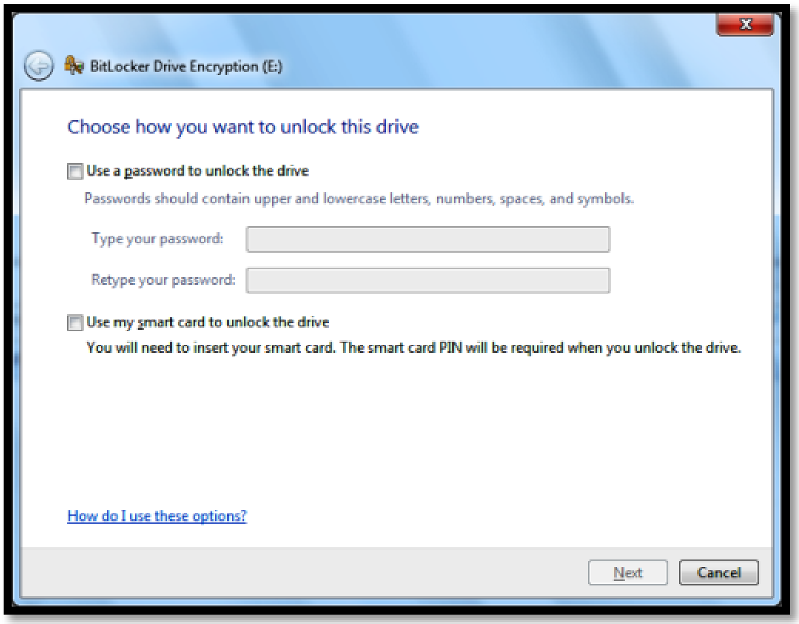

BitLocker Drive Encryption (E:)
What are BitLocker's system requirements?
Cancel

Starting BitLocker

Please wait while BitLocker initializes the drive.

Do not remove your drive during BitLocker setup.

e. When the USB Memory Stick initialization has been completed, BitLocker To Go will prompt you for a password or smart card to unlock the drive. For your purposes, you should select the “Password” option and enter a strong password or passphrase.



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

Type your password:

Retype your password:

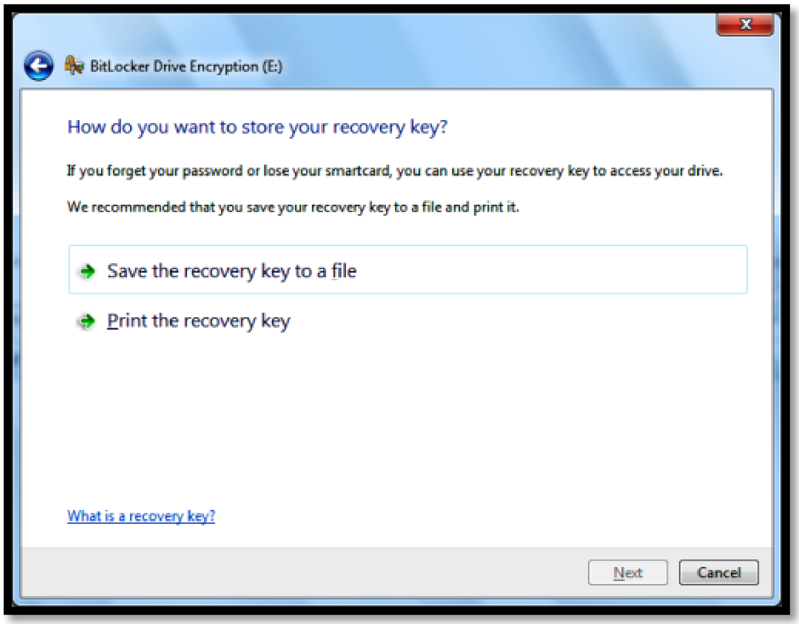
□ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?

f. After providing a strong password or passphrase, you will be prompted for a location to store your recovery key. The recovery key will help you unlock the drive if you forget the password.

g. It is recommended to save the recovery key to a file on your network drive. Once the key file has been saved you will be prompted to begin the encryption process.



BitLocker Drive Encryption (E:)

How do you want to store your recovery key?

If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

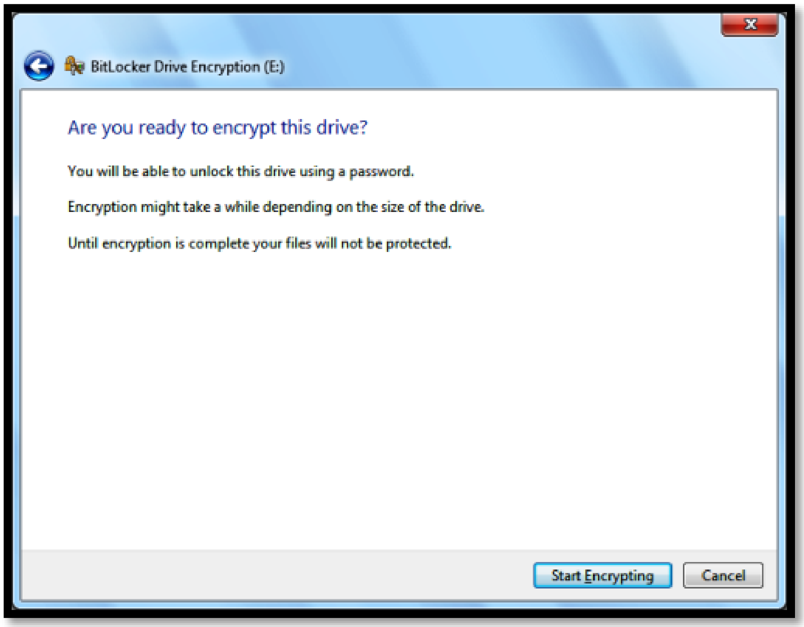
We recommended that you save your recovery key to a file and print it.

→ Save the recovery key to a file

→ Print the recovery key

What is a recovery key?

h. Select “Start Encrypting”.



BitLocker Drive Encryption (E:)

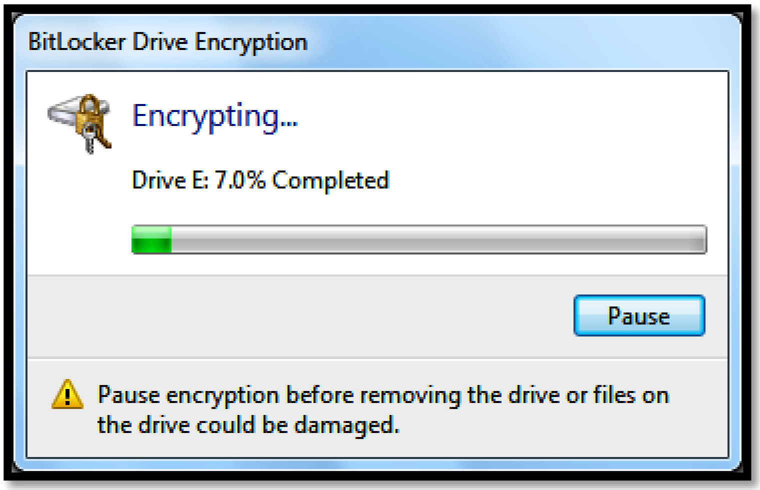
Are you ready to encrypt this drive?

You will be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete your files will not be protected.

i. While the USB Memory Key is being encrypted a progress monitor will display the progress of the operation. The amount of time the encryption takes will depend on how large the USB Memory Key is. Please note there is a pause button that allows the process to temporarily stopped if you need to perform another task.



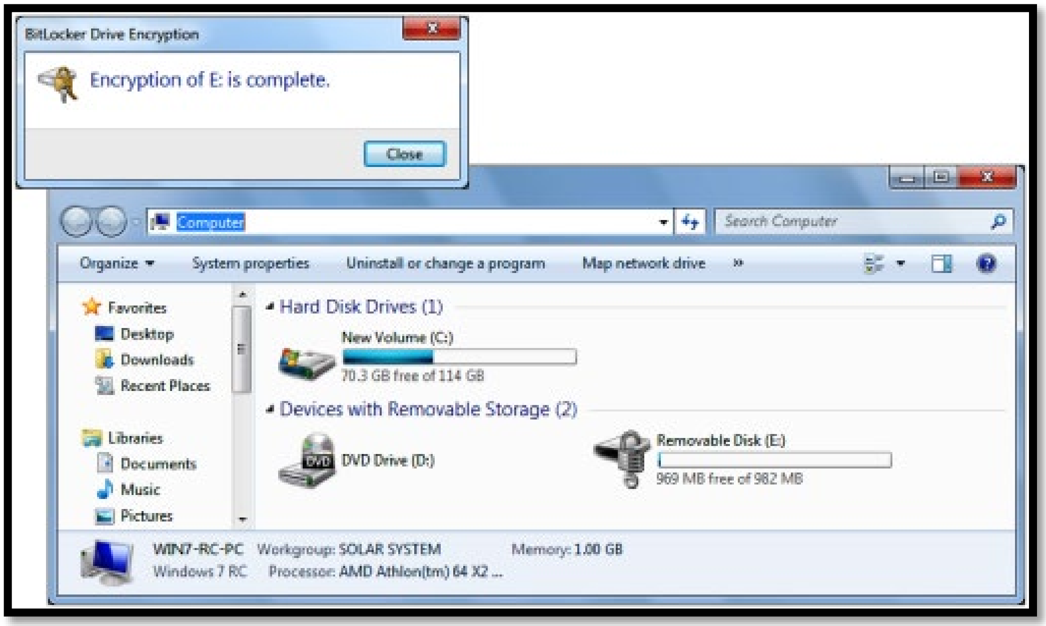
BitLocker Drive Encryption

Encrypting...

Drive E: 7.0% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

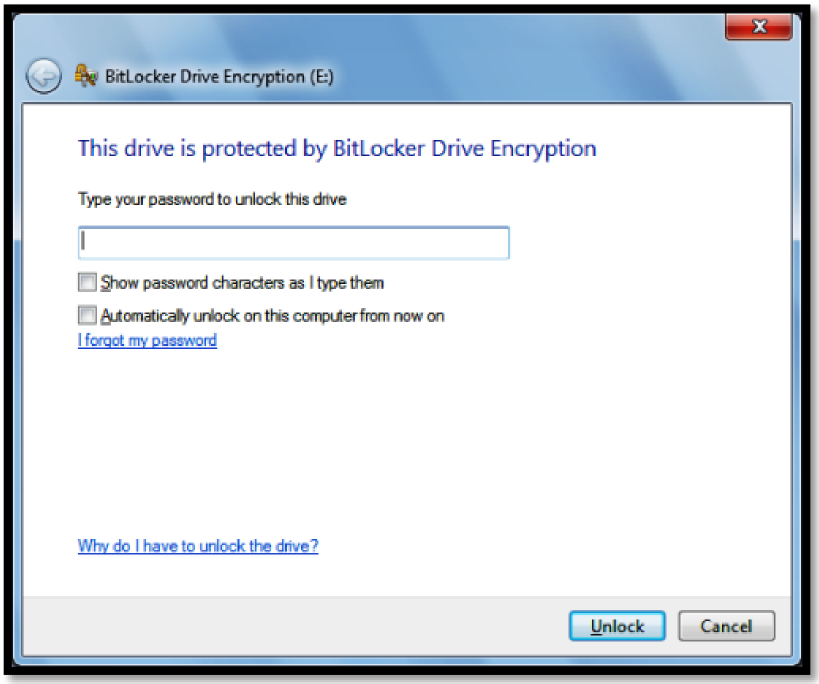
j. Once the encryption process has completed, BitLocker To Go presents you with the confirmation screen and changes the icon for your USB Memory stick.



BitLocker Drive Encryption

Encryption of E: is complete.

k. The next time the USB Memory stick is inserted into a Windows PC, you will be prompted to supply the password. Once the password has been successfully provided, select “Unlock”.



BitLocker Drive Encryption (E:)

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?

l. Now the files being stored on the USB Memory Stick are available for editing or for storing additional information on the Memory Stick.

Appendix A – Hardware Encrypted USB Memory Sticks/Drives

Hardware Encrypted USB Memory Sticks/Drives					
Product	Version	Windows	Mac	Linux	Availability
Imation Powered by IronKey	Personal, Basic or Enterprise versions	Y	Y	Y	http://www.imation.com/en-CA/
Kingston DataTraveler Vault	Privacy Edition, (4000, 5000 or 6000)	Y	Y	N	http://www.kingston.com/us/usb/encrypted_security
Kanguru Defender Series	Basic or V2	Y	Y	N	https://www.kanguru.com/index.php/catalog/category/view/id/53
	Elite or 2000	Y	Y	Y	

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Encryption Requirements standard