Encrypting your external USB drive on Windows

To prevent your important or personal information from falling into the wrong hands, you can easily encrypt the files on your USB-drive with a password. Windows, OSX and Linux all have their built-in encryption tool. This built-in encryption works on all computers with the same operating system. After encryption, only the person knowing the right password can read and change the files on your USB-drive. This quick reference describes how to use encryption on a Windows system.

NOTE: The ISSC cannot help you with decryption of your files if you forget your encryption password.

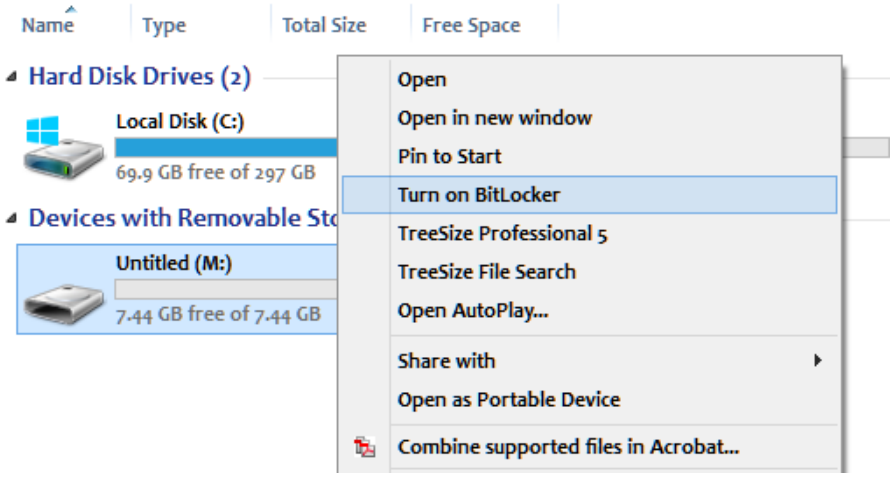
Microsoft Windows BitLocker

BitLocker is Windows' built in *encryption* software, which is available on the ISSC Windows work place and every Windows Pro, Ultimate, Enterprise or Education version after Windows 7.

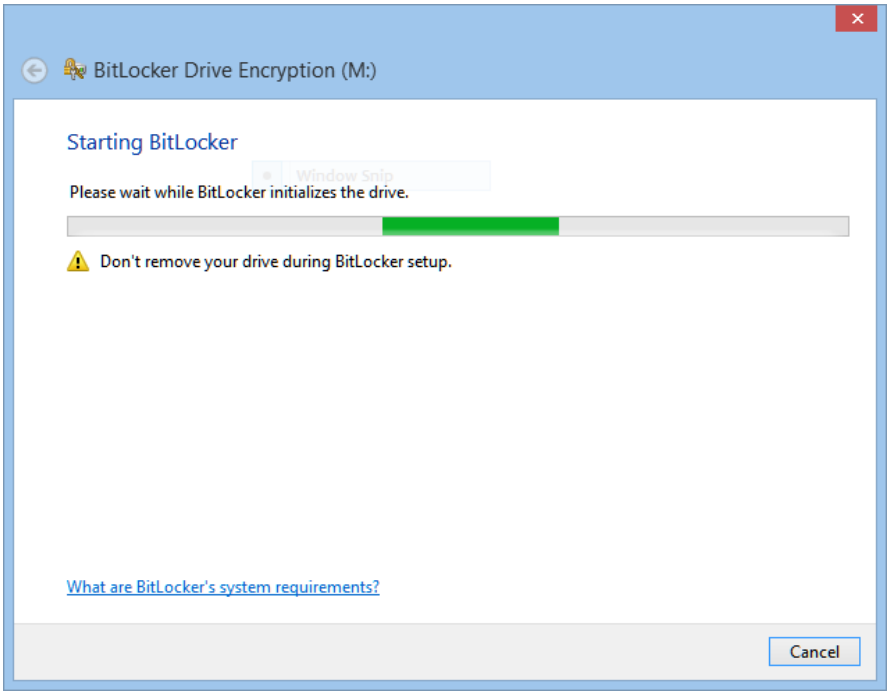
Decryption of a Bitlocker encrypted USB-device is also possible on Home versions of Windows 7, 8, 8.1 and 10. Older Windows versions can also read files from your bitlocker encrypted USB drive with Bitlocker to Go (https://support.microsoft.com/en-us/kb/970401).

This guide will be using Windows 8 but the directions are mostly the same on all Windows systems.

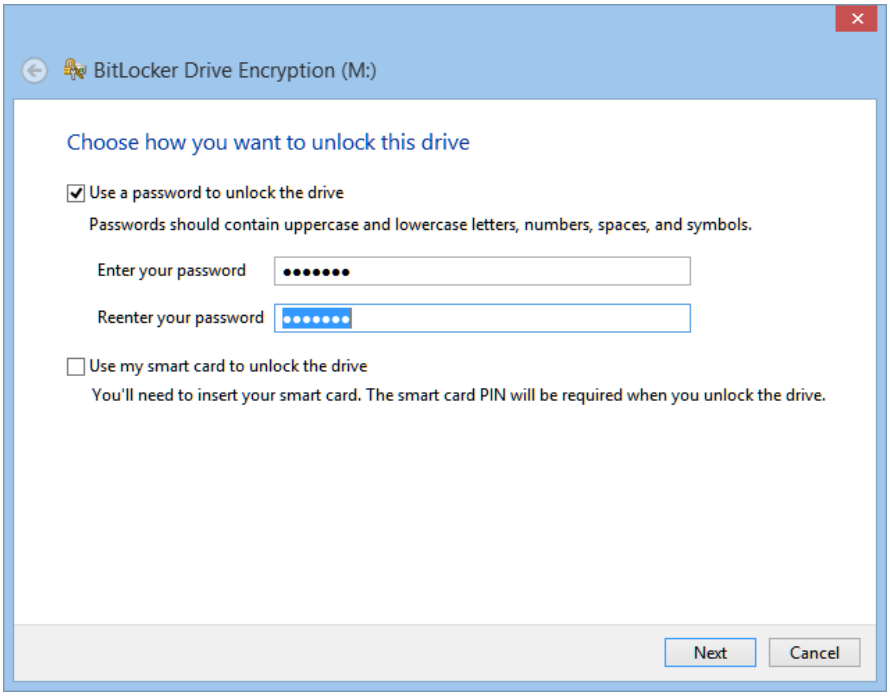
1. Insert your drive, find it either in your sidebar in Windows Explorer, or in your Computer menu and right click it. From there, select Turn on BitLocker.



You will be greeted by the BitLocker screen.

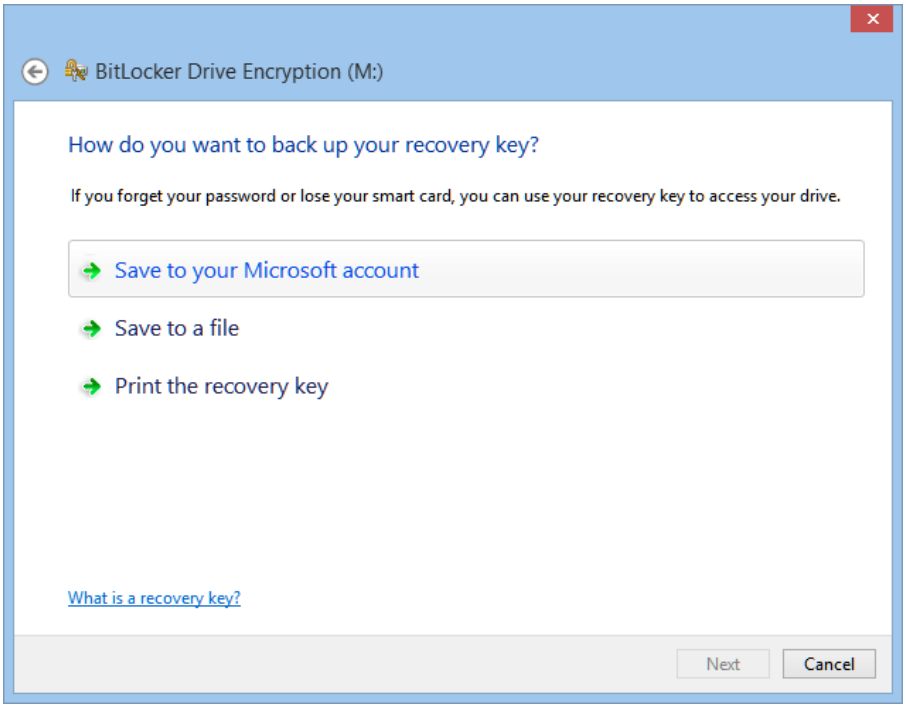


2. You can now select options to encrypt your drive. We will be using password protection today.

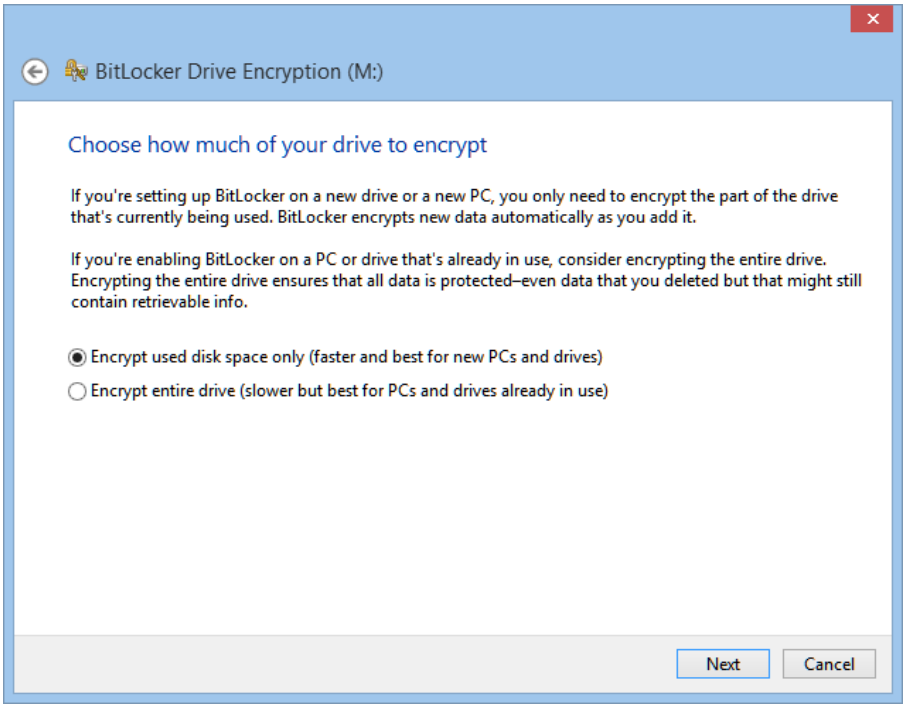


Note: Your password MUST include an uppercase letter, a lowercase letter, and a number to be compatible.

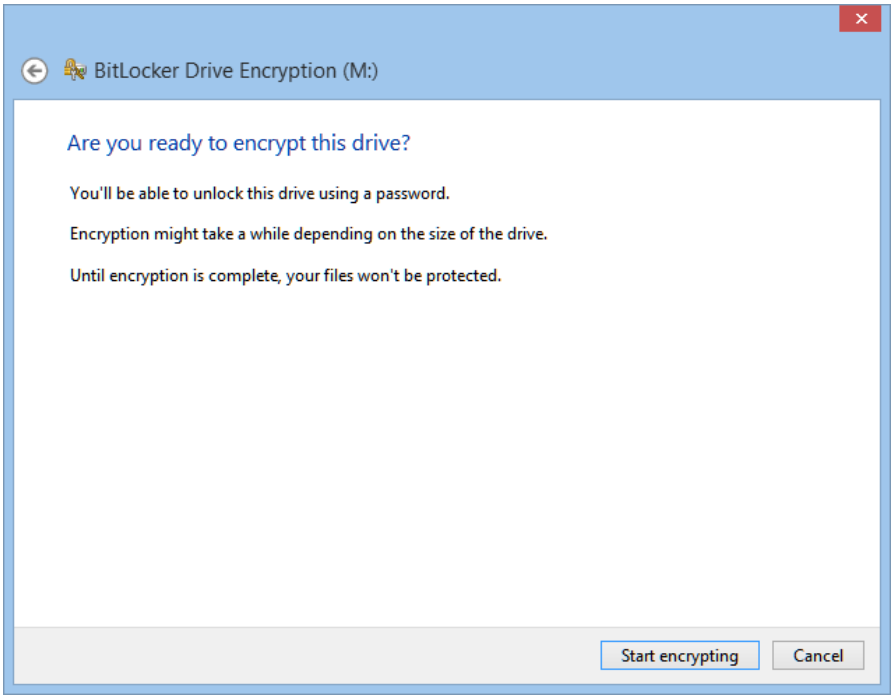
3. Click next when you're ready to continue.



BitLocker also requires you to backup a recovery key which can be used to recover the data from your flash drive if it ever happens that you forget your password. You must perform this step in order to continue.



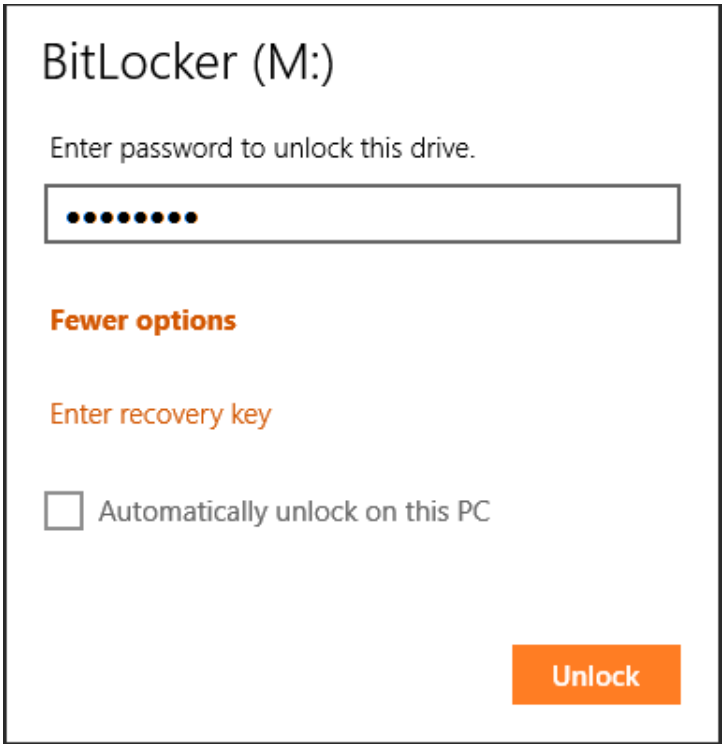
These two options allow you to either format the drive and encrypt it quickly, or perform a slower encryption which will attempt to retain any data contained in the drive.



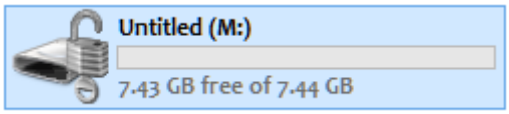
You are given a small summary page before you are asked to continue, if any of these options are not to your liking simply press Cancel and start the process again.

The speed of the encryption depends on the size of the drive and which encryption option you chose. An 8GB drive took about 2 minutes to encrypt.

Now if you remove and insert the hard drive you will be asked to enter a password, or you can enter a recovery key and have Windows automatically unlock the drive every time you insert it into the PC.



When you unlock the drive, it should look like this in your Computer.



To remove the encryption simply right click on the unlocked drive and select Manage BitLocker from where you have several options, one of which is Remove password from this drive.

Multi platform encrypting application

If the default operating system encryption methods don't work for you or if you need multi platform encryption, we recommend a tool like VeraCrypt or BoxCryptor Portable:

- https://veracrypt.codeplex.com/releases/view/619351
  This open source encryption tool replaces the once popular TrueCrypt and is available for Windows, OSX and Linux.

- https://www.boxcryptor.com/en/boxcryptor-portable-download
  A commercial encryption tool with a free version for local, portable installation (Windows, OSX, Linux) on one or two devices.

NOTE: You can have Veracrypt installed on a standard Windows work place via the application form 'Request software'. You may install VeraCrypt or BoxCryptor yourself on any PC where you have administrator rights. (This means you can not install these programs on a standard Mac or Linux work place).

This Quick reference was adapted from:

- an on line manual by Syracuse University https://answers.syr.edu/x/HIOoAQ .