Using Kingston DataTraveler Locker+ encrypted USB memory sticks

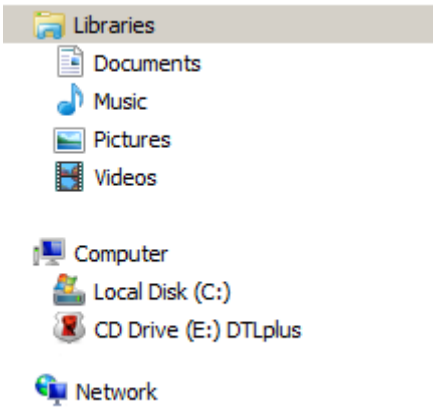
Encrypted USB memory sticks are available from the ITS service desk, and can be used to keep mobile data secure. These instructions have been tested on Windows Vista, Windows 7 and Windows 8.

Key points

- If you forget your password, the only way to regain use of the memory stick is to format it, thus wiping all data. There is no password recovery option.
- After ten unsuccessful attempts at entering the password, the stick will be formatted automatically and will have to be set up again – this means if somebody finds the stick they can still use it (by forcing it to format and then setting up a new password), but will have no access to the data without the password.
- The memory stick only works on MacOS and Windows.
- The memory stick is no more or less suitable for backups than any other memory stick, as the data is not protected from deletion/read only, so can still be deleted and will be deleted if the password is entered incorrectly ten times.
- The setup files, instructions etc are stored on a 10MB 'read only' partition and therefore cannot be deleted. The useable part of the stick is made up of a separate 4GB encrypted partition. The stick cannot be 'converted' to be used as a regular USB memory stick.

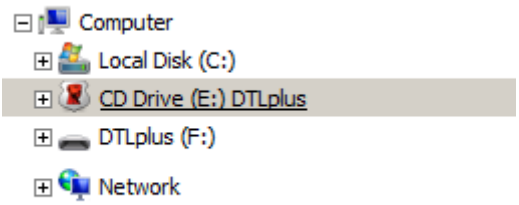
Initial set up

Plug the USB stick into your PC, and if autorun is enabled the DTL+ Setup Wizard will automatically launch; if autorun is disabled, open Explorer and select the CD drive titled 'DTLPlus' and run 'DTLplus_Launcher'.



- Choose the desired language and set up a password (and hint if required). The password has to be between six and sixteen characters long, and contain at least three of the following: upper case letters; lower case letters; numbers and special characters.

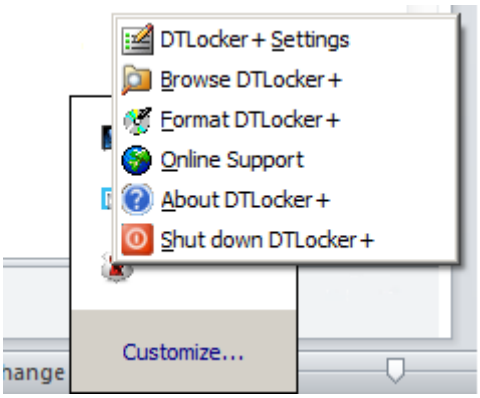
- You can then enter a name, company and some ‘Details’ which can be used to enter information visible to someone who finds the memory stick, such as contact information etc.
- The stick will then be formatted and ready for use. It will display as a regular USB stick would in Explorer as ‘DTLplus’.



From here on in, every time you insert the stick in to a PC without autorun enabled, you will have to choose ‘DTLPlus’ and then run ‘DTLplus_Launcher’ and enter the password.

Using the stick/options

One you have plugged in the stick and run ‘DTLplus_launcher’ (or let it autorun) you can find various options in the system tray:



DTLocker+ Settings - Allows you to set a new password, change the password ‘hint’, change your contact information and details and change the language settings.

Browse DTLocker+ -Opens the ‘DTLplus’ drive in Windows Explorer

Format DTLocker+ -Allows you to format the encrypted partition (the setup files and instructions remain unaffected), the password is required to do this – although entering the password incorrectly 10 times will have the same effect.

Shut down DTLocker+ - This has the same effect as ejecting the USB stickkey from via the system tray. There is nothing in the guidance that says you should use this over Windows’ standard eject. After doing this you will have to remove the USB key from your PC and reinsert it in order to use it again.