MAKE TRUECRYPT TRAVELLER MODE WORK WITHOUT ADMIN RIGHTS

By Default TrueCrypt cannot run on a USB stick (Traveller mode) without administrative rights or without the TrueCrypt software being installed on the PC.

The reason for this is that non-admin users do not have the necessary permissions to load/unload device drivers for equipment such as USB sticks. In addition a non-admin user cannot map a drive letter of which TrueCrypt needs two: one for the USB device and one for the mounted encrypted volume.

The issues are therefore:-

How to make TrueCrypt run for a user without admin rights

How to work around the mapping a drive letter problem

How to make the use of a TrueCrypt USB drive as seamless as possible for the end user

All the above are possible by combining some simple tweaks to TrueCrypt and your PC.

Step 1 – Create a TrueCrypt encrypted container on your USB drive

Step 2 – Mount the USB drive in a folder on your PC

Step 3 – Create a shortcut with elevated rights to open the encrypted container

STEP 1 – CREATE A TRUECRYPT ENCRYPTED CONTAINER ON YOUR USB DRIVE

1. Create a folder on your USB drive called **System**.
2. Run the TrueCrypt set up program and choose the Extract option. Extract to the System folder on your USB drive.
3. From the System folder you've just copied to the USB stick run **TrueCrypt Format.exe**
4. Choose **Create a file container**, click **Next**
5. Choose **Standard TrueCrypt volume**, click **Next**
6. Click **Select File** and browse to the root of the USB stick
7. Type in the filename **MyData**, click **Save**, click **Next**
8. Leave the default encryption Algorithm as **AES** and click **Next**
9. Enter a Volume Size (preferably equal to all of the remaining space on the drive if you don't want your users accidentally writing to an unencrypted part of the USB stick).
10. Enter a password for the encrypted container, move your mouse around the TrueCrypt window for a while to help randomize the creation of the encryption key then click **Format**. On a 1GB key this should take about 2 or 3 minutes. Once complete click **Exit**

STEP 2 – MOUNT THE USB DRIVE IN A FOLDER ON YOUR PC

Since generally a user without admin rights won't be able to have their USB stick select the required drive letters for TrueCrypt to run we can use the option in Windows to mount a USB device in an NTFS folder:-

1. Logged in as a user with admin rights create a folder on the C: drive called **Mount**. Inside create a folder named with the username of the user who will use the encrypted stick.

2. Logged in as the restricted user browse to C:\Windows\System32 and right-click MMC.exe. Select RunAs and select an account with admin rights. Enter your password to run the MMC and add Disk management snap in.

3. For the USB device that's running TrueCrypt right-click and select **Change Drive Letter and Paths**.

4. Remove the assigned letter for the drive then repeat step 3 and click **Add**. Here you'll select "**Mount in the following empty NTFS folder**" then browse to the folder your created in step 1 inside the C:\mount folder.

STEP 3 – CREATE A SHORTCUT WITH ELEVATED RIGHTS TO OPEN THE ENCRYPTED CONTAINER

Since TrueCrypt will not run without admin rights, in the next step we're going to create a shortcut to the TrueCrypt container we've already created on the USB stick. We'll use the standard Windows RunAs syntax in the shortcut to store admin credentials which will allow a user to run the shortcut in future without admin intervention.

TrueCrypt has all sorts of switches offering various ways to customise this step but here's what I did to make it work

1. Right-click to create shortcut on the desktop and point it to the TrueCrypt.exe file in the System folder on the USB stick which now resides in C:\mount\%username%

2. Edit the path of the shortcut to the following (where xpclonesp3 is the name of the local computer):-

C:\WINDOWS\system32\runas.exe /user:xpclonesp3\administrator /savecred "C:\Mount\%username%\System\TrueCrypt.exe /v c:\mount\%username%\mydata /lv /a /m rm /b /q background"

3. The first time you double click this shortcut you'll get a command prompt window asking for the password of the local administrator. Type it in and press return, you'll then get the TrueCrypt password prompt. After successfully entering the password you'll have a mapped V: drive to the encrypted container on the USB stick. For an explanation of the components of the above path click here.

4. You'll want to change the icon for the shortcut after adding the extras in the path so choose either the TrueCrypt icon or other suitable icon image.

The function of the various TrueCrypt switches in the path can be found here under the command line usage section:-

http://www.truecrypt.org/docs/

KNOWN ISSUES AND TIPS

It’s not possible to use the TrueCrypt /e switch, it doesn’t stop mounting the container but produces an error message and doesn’t automatically open Windows Explorer.

It’s not possible to use the %computername% variable in the shortcut path

Make sure you dismount the encrypted container fully before removing it the data can become corrupted/unreadable/unrecoverable

Use up all of the space on the USB stick when created the encrypted container if you don’t want your users to accidentally write to the unencrypted part.

A single USB stick cannot be mounted for multiple user accounts on the same PC. Once you use the C:\mount\username folder that path is tied to that individual USB device

A single user account can use multiple USB sticks but you’ll need to mount them in separate folders and won’t be able to use the %username% variable in the path for additional sticks. Instead create a folder for each stick in the mount folder and in the shortcut path for TrueCrypt point it at that location.

Automating this process

In order to make this process a little easier you can create the TrueCrypt shortcut and just copy it to multiple PCs. Then just change the computer name in the shortcut’s path.