How to enable Disk Encryption on a laptop

Skills and pre-requisites
Intermediate IT skills required. You need to:

- have access to, and know how to change settings in the BIOS
- be confident that your data is backed up
- have local administrator access
- be familiar with the Data Protection concepts covered in the university’s regulations regarding laptops.

If you will need help, or for us to do this for you (there may be a charge for this service), contact us: www.kent.ac.uk/itservices/help/

Trusted Platform Module (TPM)
A TPM is a device inside your laptop used to securely and conveniently store the keys used to (among other things), encrypt the information on disks. They are not standard on “consumer” devices but are the best way to manage your digital credentials if it has one. If it is a “business” grade laptop and purchased in the last few years, then it probably does have one.

If your laptop does not have a TPM and your version of Windows does not support Bitlocker you should use software based disk encryption instead.

As of the 28 May 2014, the Truecrypt project appears to have ended.

We continue to recommend using Truecrypt 7.1a and this position will be reviewed in the near future. Please download Truecrypt 7.1a from http://truecrypt.ch and follow the instructions at the end of this document.
Establishing if the Device has a TPM

In order to know which method to use to encrypt your laptop, you first need to establish whether or not it has a TPM and also that the windows drivers are configured correctly. You can check in the BIOS or, as you will be using it later anyway, run the TPM management console:

Log on with your local admin account and run tpm.msc from Start\Search area:

If you have a TPM and it has not been initialised by someone else, you should see the following status information:

This is good news and you can proceed to the next section titled “Enabling your TPM”.

If the status is “The TPM is on and ownership has been taken” then you should already be in possession of the “Owner Password”. To verify you have the correct password before continuing, try turning the TPM off or on via the links in the right hand window of the TPM management console.

Assuming you can verify the Owner Password, move on to “Setting up Bitlocker”; if not, then you will need to boot into the BIOS and reset the TPM (methods and terminology will vary, but look to clear or reset the TPM). This will wipe all passwords and credentials in the TPM and allow you to start from scratch as detailed below.

If you get the following screen then your laptop probably does not have a TPM:
HOWEVER, there are two things to try before using software encryption.

1. Some BIOS setups allow the TPM to be disabled or hidden from the OS. Please do check through all the security settings available to you in the BIOS and refer to the manufacturer’s documentation if necessary.

2. It may be that the windows driver is not configured correctly. To check this, run the Computer Management console (compmgmt.msc), from the search area and go to device Manager:

![Computer Management Console](image)

This will clearly display either an unknown device (for which you need to get drivers from the manufacturer as windows doesn’t have them), or quite often the manufacturer driver doesn’t work properly. If you uninstall the manufacturer driver and let windows install its own, it quite often works better.

If you have been through all this and it definitely does not have a TPM, you can still encrypt your disk(s), please go to the section below entitled **Using TrueCrypt to Encrypt Disks**.
Enabling your TPM

The first thing to do is turn your TPM on and configure it to accept your keys.

Before you go any further, now is the time to ensure that all data currently held on your laptop is indeed stored elsewhere. Laptops should not be treated as a permanent location for files, they should be thought of just as a way of temporarily taking documents away from their usual secure and regularly backed-up location (probably a network drive or SharePoint etc.).

IMPORTANT: If it is not done properly, changing anything in the TPM or encrypting data can result in the complete and unrecoverable loss of the data on your laptop.

1. Backup your data and verify that it is a usable backup.
2. As detailed previously, log on with your local admin account and run tpm.msc from Start\Search area.
3. Select “Initialize TPM” option as shown below:

![TPM Management on Local Computer]

4. Your machine will reboot, you will be prompted by the BIOS to confirm you wish to turn the TPM on.
5. Once you log back into windows (again with your local admin user), you should then be prompted to create the TPM Owner password. The TPM owner password/key is critical should you need to perform any data recovery in the future and should be carefully safeguarded. I would suggest that you obtain the smallest capacity, cheapest USB flash drive and dedicate it to storing your backup/recovery keys but alternatively you can print it, or even write it down, but under no circumstances should this be stored with your laptop; If it is, there is no point in encrypting your disk(s) and you will not be complying with your obligations under data protection law.
6. Choose to automatically create the password.
7. Ideally, save the password to your USB device but you could print it, or carefully write it down (not recommended). It will suggest a filename of machinename.tpm, probably best to stick with this.
8. You can then click the “Initialize” button and your TPM will be ready for use.
**Setting-up Bitlocker**
Although your machine may come with its own, perfectly acceptable, encryption software we suggest you use BitLocker so that the solutions in use are kept to a minimum and are therefore more familiar to us.

Before you go any further, now is the time to ensure that all data currently held on your laptop is indeed stored elsewhere. Laptops should not be treated as a permanent location for files, they should be thought of just as a way of temporarily taking documents away from their usual secure and regularly backed-up location (probably a network drive or SharePoint etc.).

**IMPORTANT:** If it is not done properly, changing anything in the TPM or encrypting data can result in the complete and unrecoverable loss of the data on your laptop.

1. Backup your data and verify that it is indeed a usable backup.
2. Log on as local administrator.
3. Open the BitLocker configuration screen in control panel:

   ![BitLocker Configuration Screen](image)

4. Click on “Turn on BitLocker” next to your C: drive. NOTE: If you have a separate data disk(s) you will need to enable the encryption on them individually.

9. Ideally click “Save the recovery key to a USB flash drive”. As mentioned previously, It is suggested that you obtain the smallest capacity, cheapest USB flash drive and dedicate it to storing your backup/recovery keys, but alternatively you can print it, or even write it down, but **under no circumstances should this be stored with your laptop**; If it is, then there is no point in encrypting your disk(s) and you will probably not be complying with your obligations under data protection law.

5. Once you have selected your USB drive and saved the recovery key to it you are almost ready to begin.

It is worth clarifying that your USB device should now contain two important pieces of information.

- Your TPM Owners key (*machinename.tpm*, used to manage the TPM and all credentials stored in the TPM).
- Your C: drive recovery key (*Similar to: BitLocker Recovery Key GGPL8E6C-0E33-4618-8C9Y-C84U1A6786D2.TXT*, used to decrypt your drive should anything go wrong with your laptop).
6. Click next and then tick the “Run BitLocker system check” box and click Continue.

7. You will then see the following confirmation and reminder, ensure your USB is inserted and click restart now.

8. It will restart and check that all is well with the boot process before it starts encrypting.
9. You can then log back on and you will see a confirmation box and icon in your notification area while the drive is encrypted. This can take several hours but you can safely continue to work while this happens.
10. Once completed please continue on to the next section to complete the configuration.
**BitLocker Boot PIN (Not Suitable for Tablets)**

BitLocker by itself is great drive encryption, but unfortunately it has some shortcomings in its default configuration. Namely, there’s no safeguard at boot time preventing the drive from being accessed. If your computer is stolen or physically compromised, the drive is ready and willing to give access to your data.

Fortunately BitLocker supports a PIN code which has to be entered at boot time to unlock the drive.

1. Log on as local administrator.
2. Open an administrator command line (search for cmd, right click cmd.exe, click “run as administrator”). Note: This is different to launching a cmd line while simply logged on as a local administrator.
3. Run the following command: `manage-bde -protectors -add c: -TPMAndPIN`
4. You should receive output similar to the following, during which you’re prompted for your PIN (no confirmation of keystrokes will appear on the screen during PIN entry):

   BitLocker Drive Encryption: Configuration Tool version 6.1.7601
   Copyright (C) Microsoft Corporation. All rights reserved.
   Type the PIN to use to protect the volume:
   Confirm the PIN by typing it again:
   Key Protectors Added:

   If you get the following error...

   ERROR: An error occurred (code 0x80310060):
   Group Policy settings do not permit the use of a PIN at startup.
   Please choose a different BitLocker startup option.

   ... then you will need to edit the local computer policy to allow a PIN to be set by performing the following steps:

   I. Click **Start > Run** and gedit.msc
   II. Browse to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives**
   III. Open the key **Require additional authentication at startup**
   IV. Enable that Key and set **Configure TPM startup Pin** to **Require startup PIN with TPM**

   You should then be able to issue the command in step 3 above.

5. Now when you reboot you will have to enter your PIN before the encrypted disk is mounted.
   Note: You will need to enter your PIN using the Function keys (F1-F9 plus F10 as 0), rather than the usual number keys.
Final Notes on TPM

- Your disk is only truly protected when powered off, so get into the habit of shutting down.
- Encryption is only as strong as your password. Always ensure your passwords are “strong” enough (you can check [here](http://technet.microsoft.com/en-us/library/ee523219(v=ws.10).aspx)).
- Do not store any backup keys with the laptop. You will have a “TPM Owner password and also “Bitlocker Recovery Key(s)” to print or save on USB and keep somewhere reasonably secure and away from the device.
- Information on using your recovery key to unencrypt a drive can be found here: http://technet.microsoft.com/en-us/library/ee523219(v=ws.10).aspx

As your disks are now encrypted you do not need to read past this point.
Using TrueCrypt to Encrypt Disks

Although your machine may come with its own, perfectly acceptable, encryption software we suggest you use TrueCrypt so that the solutions in use are kept to a minimum and are therefore more familiar to us.

TrueCrypt is free, open source, has a good reputation and is widely adopted. You can download the “latest stable version” from here: http://www.truecrypt.org/downloads

Before you begin please read the following caveats:

- TrueCrypt does not contain any mechanism or facility that will allow partial or complete recovery of your encrypted data without knowing the correct password. Should you forget the password it will not be possible to recover the data.
- Make sure that you have a backup copy of the files on your laptop before starting (not stored on the laptop).
- Prior to using, you will have to create a TrueCrypt Rescue Disk. So you will need a CD/DVD drive and blank media. Your TrueCrypt rescue disk is unique to your machine, so do not lose it. If your machine does not have a built in DVD/CD then you will need to borrow an external device.
- By restoring key data using a TrueCrypt Rescue Disk, you also restore the password that was valid when the TrueCrypt Rescue Disk was created. Therefore, whenever you change the computer’s encryption password (not to be confused with your logon password), you should destroy your TrueCrypt Rescue Disk and create a new one.
- Note that even if you lose your TrueCrypt Rescue Disk and an attacker finds it, he or she will not be able to decrypt the system partition or drive without the correct password.
- The encryption key is held in RAM while powered on (or sleeping), also saved in hibernation file.
- TrueCrypt does not support Dynamic Disks.
- Do not store your computer’s encryption password with the computer. Do write it down and keep somewhere reasonably secure but away from the device.
Encrypting Your Disk (Including C: or System Drive)

**Preparation**

1. Backup your data. Before you go any further, now is the time to ensure that all data currently held on your laptop is indeed stored elsewhere. Laptops should not be treated as a permanent location for files, they should be thought of just as a way of temporarily taking documents away from their usual secure and regularly backed-up location (probably a network drive or SharePoint etc.).

2. Log on as an admin account.


4. Click Download

5. Save as...

6. ...and save to your desktop

**Installing TrueCrypt**

1. Still logged on as your admin account, right click on the setup file downloaded to your desktop, select run as administrator and confirm the UAC prompt.

2. Run through the install wizard accepting all defaults (Accept licence, next, next, install, ok, finish and yes to reboot the machine).
3. Once rebooted run TrueCrypt from the desktop or start menu.

4. Select Encrypt System Partition/Drive from the System menu.

5. Complete the wizard as shown:

6. The next step involves choosing a password to use as the key to your computer. Please remember that this password will be required by ANYONE who needs to log on.
   a. This password will have to be recorded, stored away from the computer and given to anyone who needs to use the computer.
   b. Encryption is only as strong as your password. Always ensure your passwords are “strong” enough (you can check here).
   c. Do not use your normal logon password.

7. Once you have selected and recorded a password, continue with the wizard as shown:

8. Next you HAVE to create a Rescue Disk (TRD). The process will not continue until you have burnt and verified the TRD.
9. Insert your blank media and continue as shown:

10. Once you have burnt your rescue disk you should remove it, label it and store it somewhere safe. If you ever have any problems with your machine resulting in the need to recover your data you will need this disk. It is unique to your machine and cannot be used without the password.

11. The next step is to test that everything is installed and working BEFORE TrueCrypt encrypts your data. You will be required to reboot your machine and enter the password you specified earlier.

12. Do not forget to remove your TrueCrypt Rescue Disk BEFORE rebooting otherwise you will be testing the rescue disk and not the software installed on your machine.

13. You should enter your password when requested.

14. Hopefully you will see the following confirmation:
15. You can then read/print the following if you wish:

16. The software will then encrypt your entire computer. This will take several hours, but you can continue to work and even reboot if need be.

17. Eventually you will see the following message:
18. Please do reboot and check that you can still enter the computer’s password and then logon.

Final Notes on TrueCrypt
- Your disk is only protected when powered off, so get into the habit of shutting down.
- Encryption is only as strong as your password. Always ensure your passwords are “strong” enough (you can check here).
- Do not store any passwords with the laptop.
- Information on using the TrueCrypt Rescue Disk (TRD), can be found here: http://www.truecrypt.org/docs/?s=rescue-disk