Enabling BitLocker encryption on Dell laptops

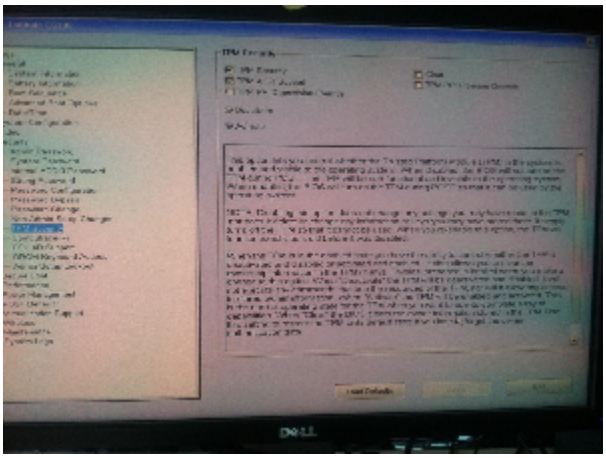
Our Dell Latitude laptops have a Trusted Platform Module (TPM) which can be used for disk encryption using BitLocker in Windows 7.

The defaults for BitLocker are pretty lame (i.e. anyone has access to the data on your laptop), so here's how to do it properly.

The goal is to have a laptop that has it's disk totally encrypted, using the TPM and a proper password.

Enable the Trusted Platform Module in the BIOS

This various in different BIOSes, this is how it looks on a Latitude E6330:



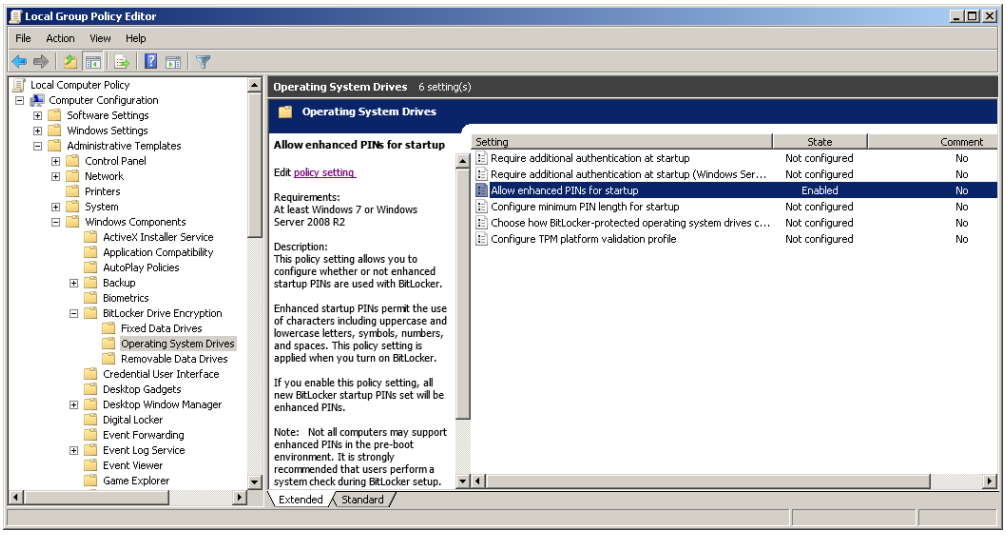
Initialise the TPM in Windows

Initialise the TPM by running **tpminit.exe**:

Let Windows create the password, and then save it to a USB stick for safekeeping.

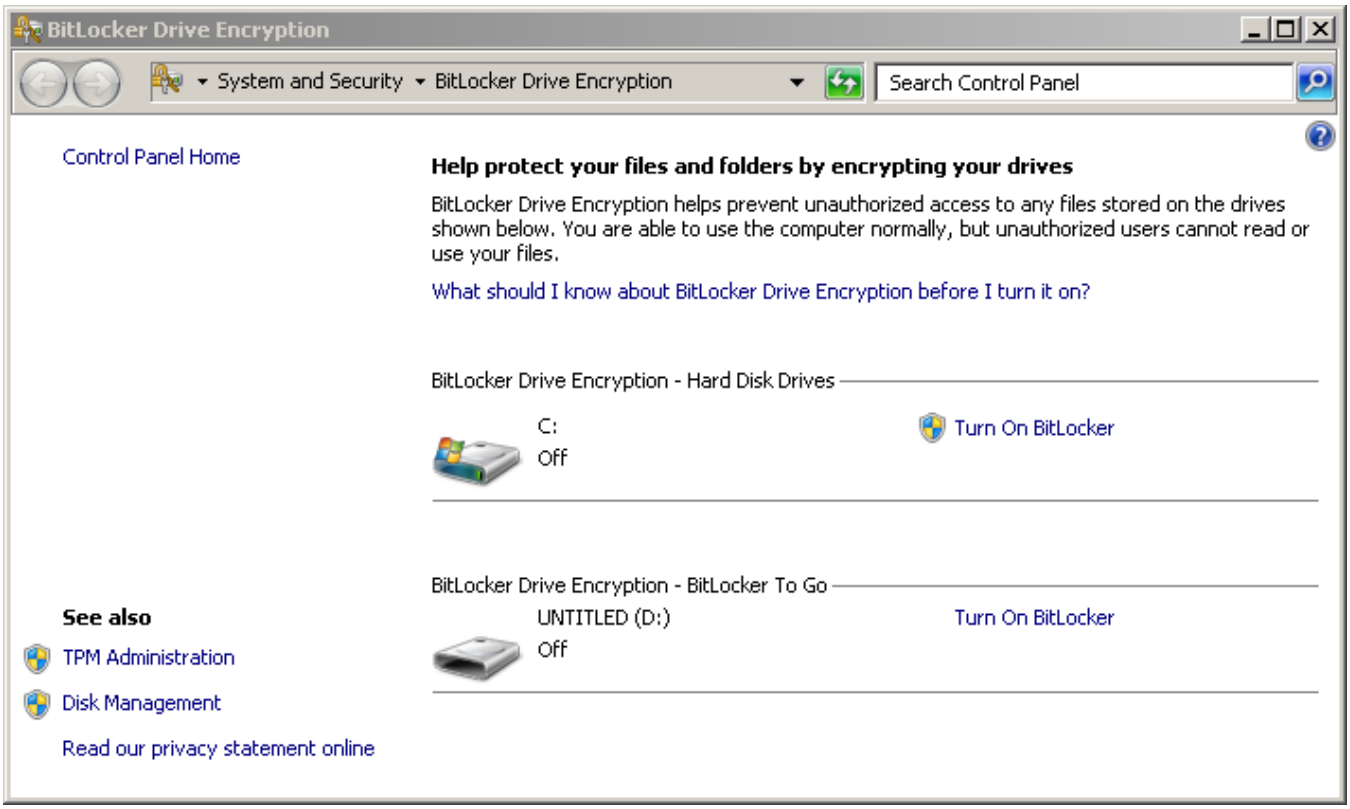
Enable non-numeric PINs

Later on we want a PIN to be required for unlocking the drive. For reasons that are beyond me Microsoft have chosen a PIN (only digits) to be the default, and not a password (any character). Obviously we want to be able to use all the characters. This is done by enabling the "Allow enhanced PINs for startup" setting in the Local Group Policy Editor (gpedit.msc):



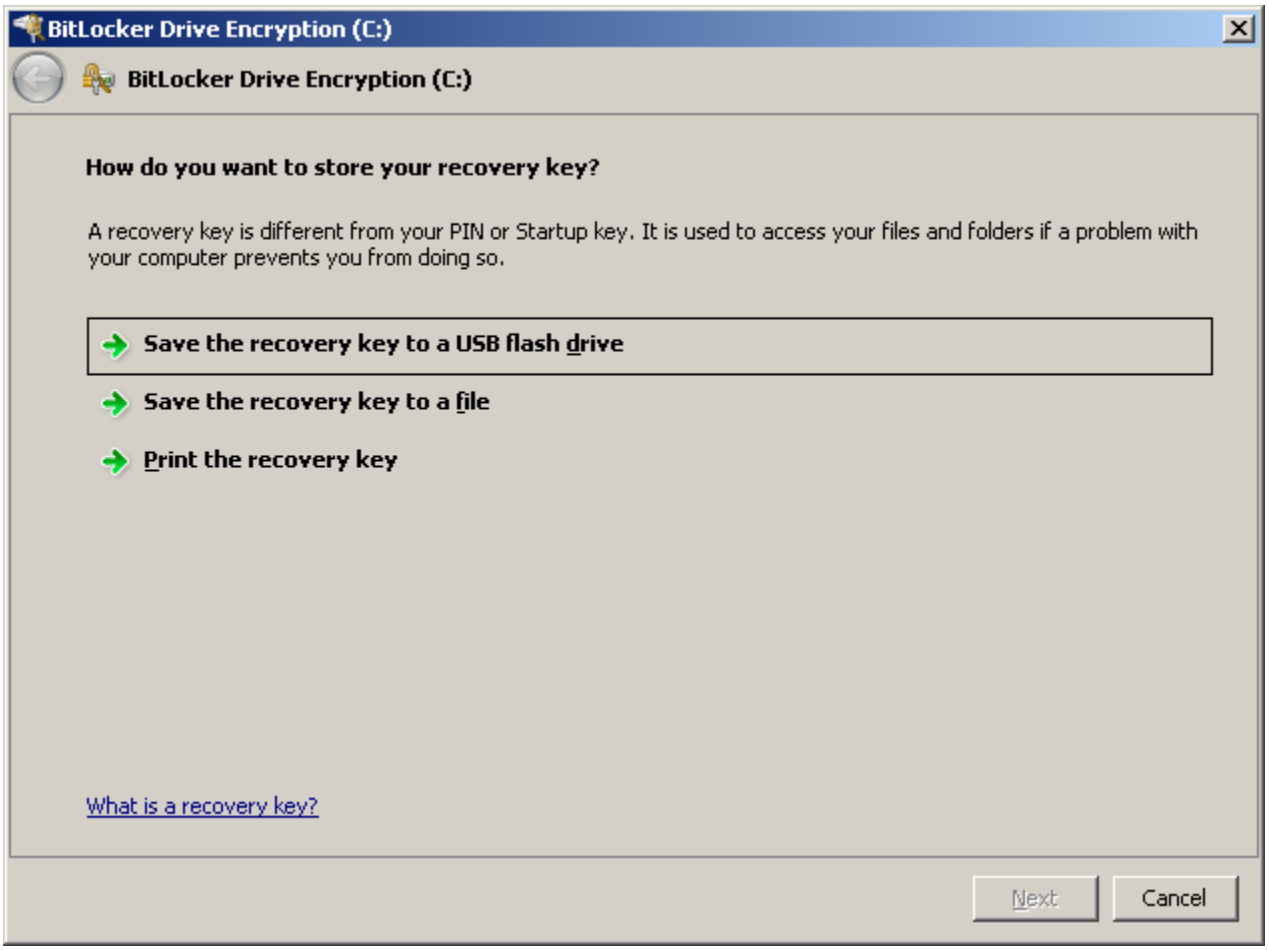
Enable BitLocker Drive Encryption

This is done through the BitLocker Drive Encryption control panel. Turn it on for the C: disk:

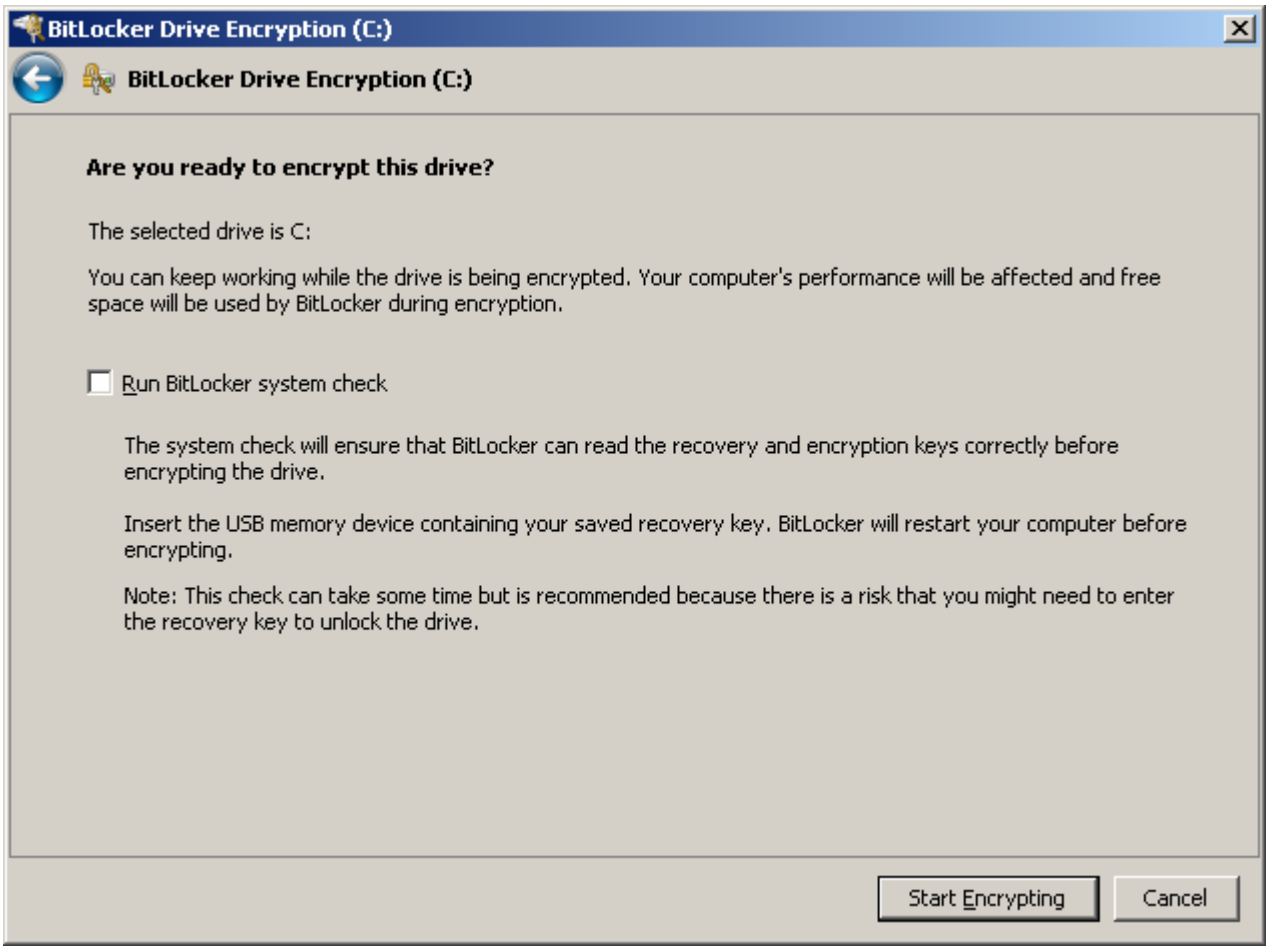


Windows will now generate a recovery key. Save a copy onto the TWO USB sticks (one backup is no backup) labelled "Bitlocker keys" in a physical key safe.

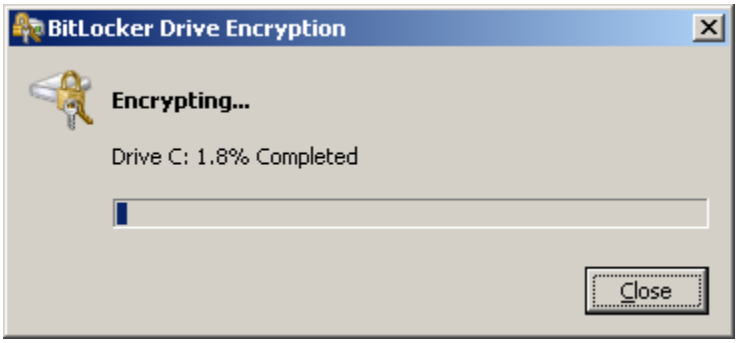
If the PIN ever gets lost/forgotten, or some boot parameters are changes, you need it to boot the computer with.



Now it's time to encrypt the drive. You can run a check to make sure your laptop really can be recovered with the key that is stored on the USB stick:



This encryption will take some time, but on a modern laptop that have a CPU that does crypto in hardware, and an SSD, it takes about 15 minutes:



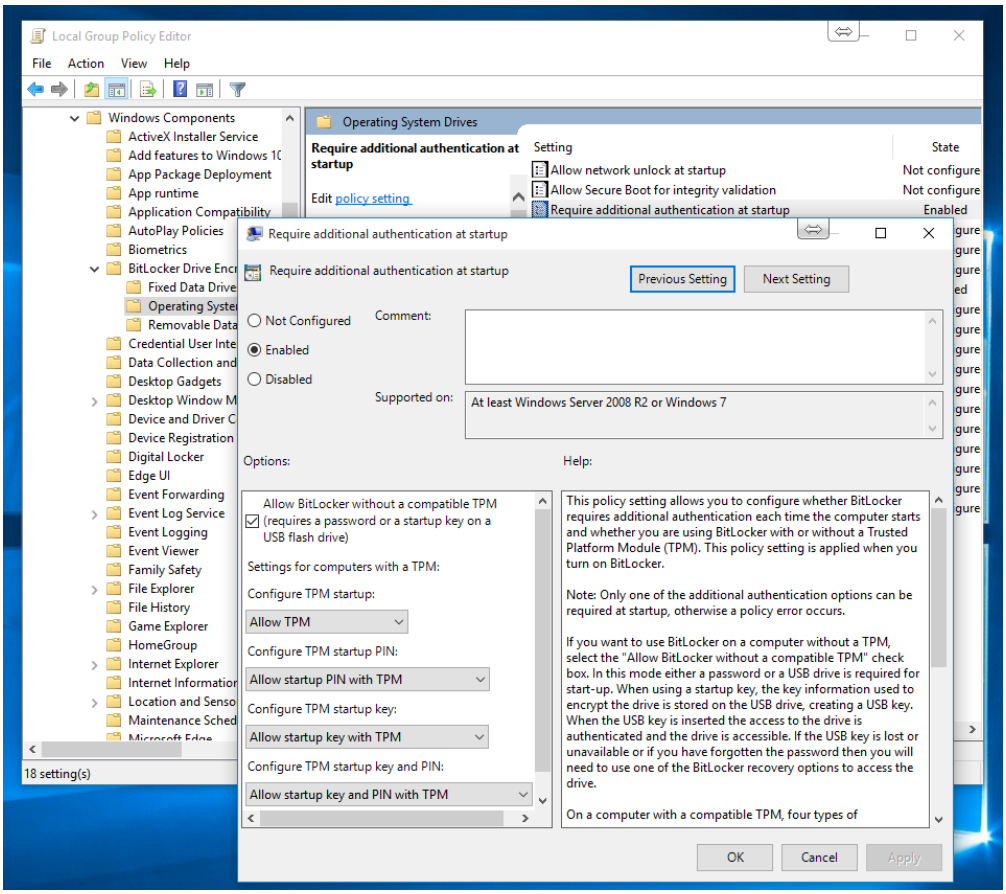
Enable the PIN code

At this moment the C: partition is encrypted using the TPM. This means that the partition is unreadable when put into another computer.

The combination of the laptop and the disk (as you have it now) does not need any authentication, so not very useful.

Run the Group Policy Editor again, and enable "Require additional authentication at startup" settings.

Also, check the "Allow Bitlocker without a compatible TPM" box:



Once this is done, you can finally configure a password (mistakenly called PIN):

```
manage-bde -protectors -add C: -tpmandpin
```

To change the PIN/password later, simply issue:

```
manage-bde -changepin C:
```

What do if you can't get in any more

Sometimes if you changed to BIOS settings, your system needs the BitLocker Drive Encryption recovery key.

Once that is done, you should suspend and then resume the BitLocker protection in the BitLocker Drive Encryption control panel.