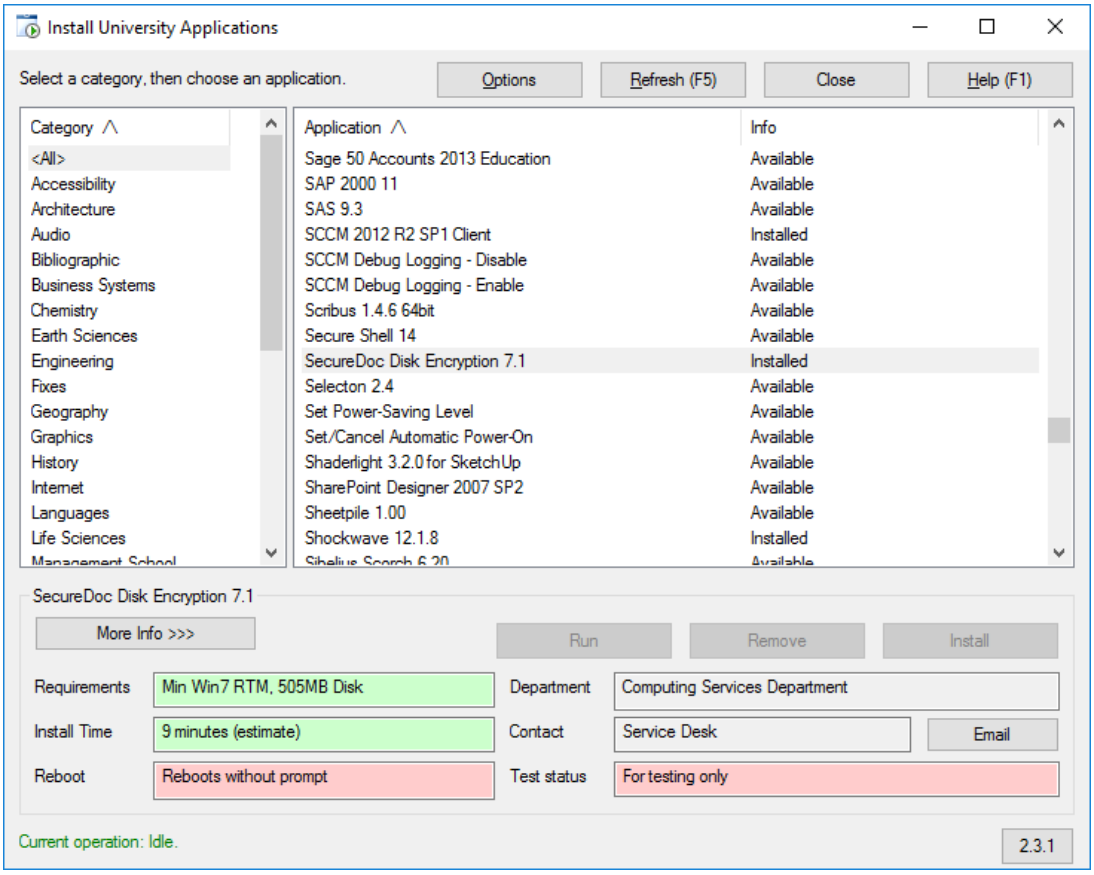
UNIVERSITY OF LIVERPOOL | COMPUTING SERVICES

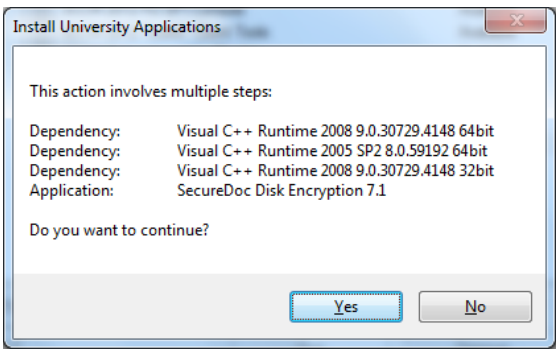
Installing SecureDoc Disk Encryption

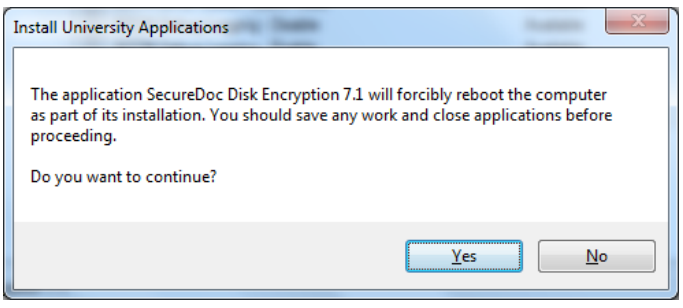
To encrypt your University MWS HP laptop, follow the step-by-step instructions:

- Make sure your laptop is connected to the mains power. The installation will not run if the laptop is on battery power only.
- On your desktop double click the icon for **Install University Applications**.
- Select the Category **<All>**
- Scroll down the list of applications and select **SecureDoc 7.1** then click **Run**.



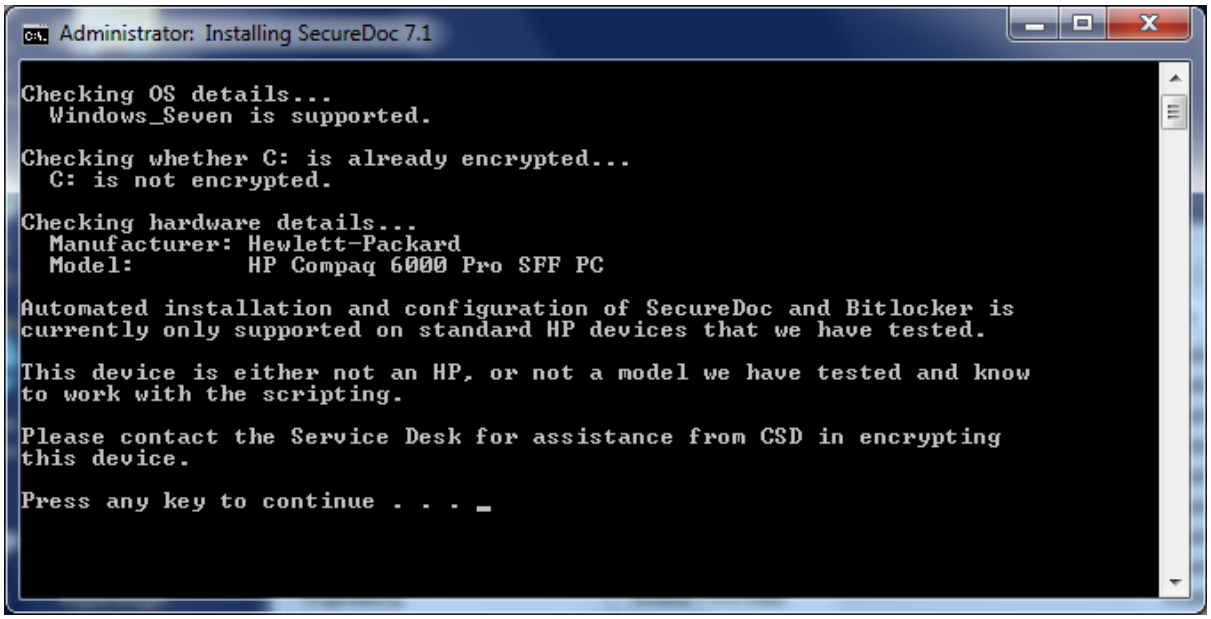
- You will see messages about the prerequisites that will be installed (the list might vary, as some users may have elements already) and that the process will involve reboots.
  Click **Yes** to continue with the installation.



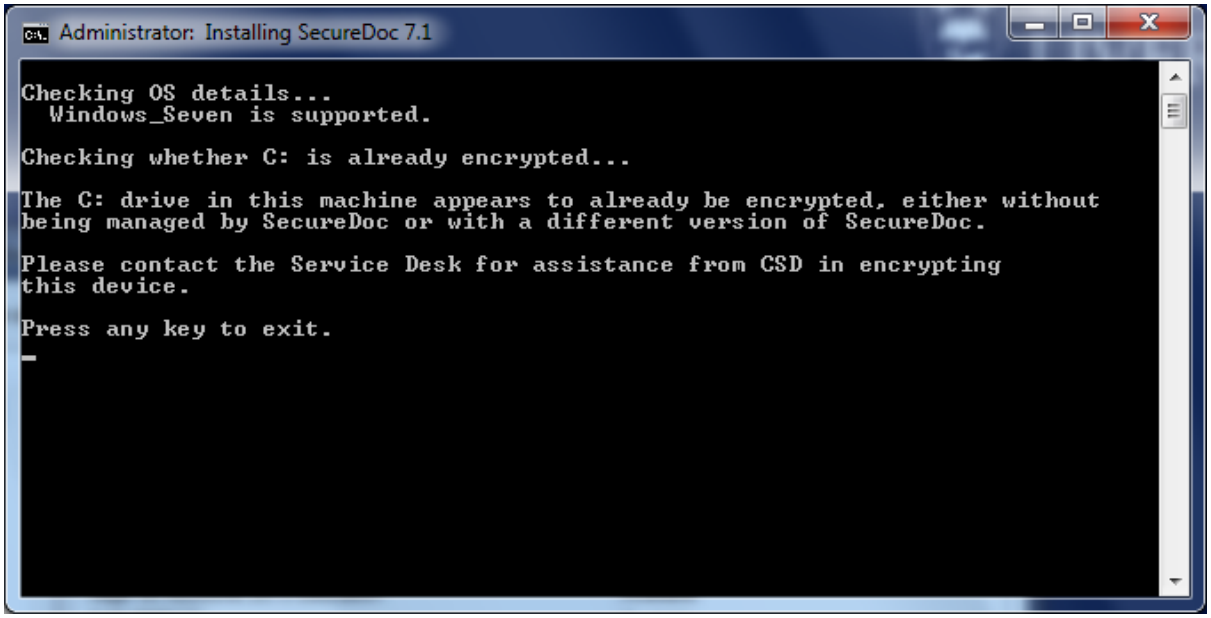


- On proceeding, the prerequisites will be installed. You may see one of the following messages:

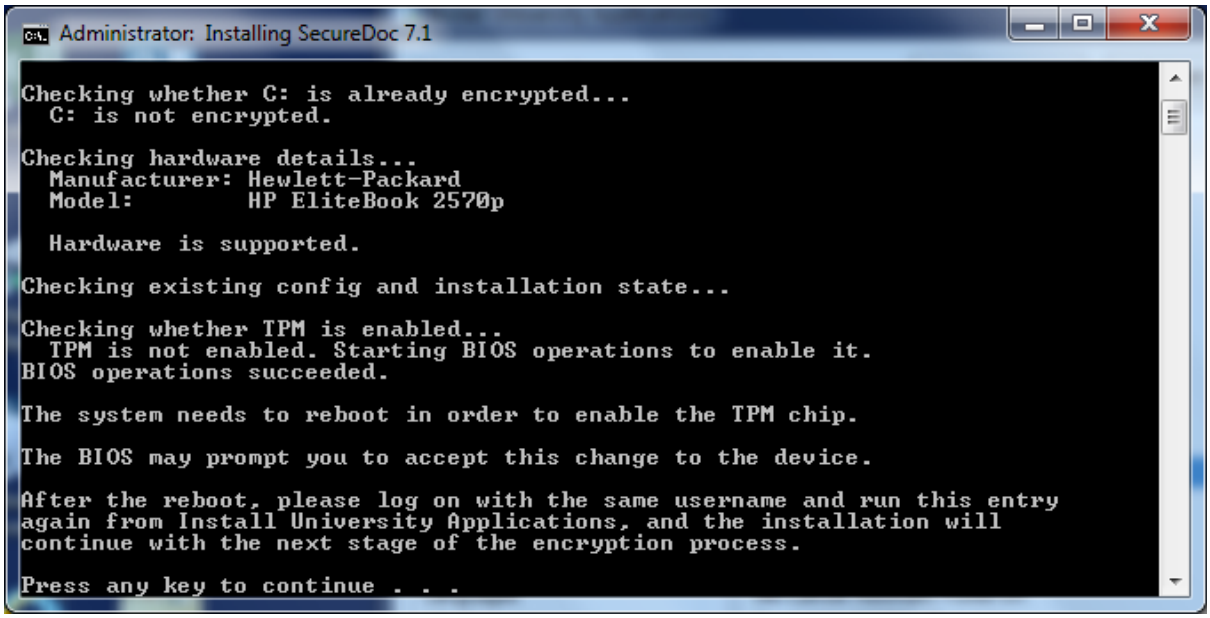
If the laptop you are using does not support the encryption software, you will see this message:



If your computer has already been encrypted by using BitLocker manually, you will see this message:



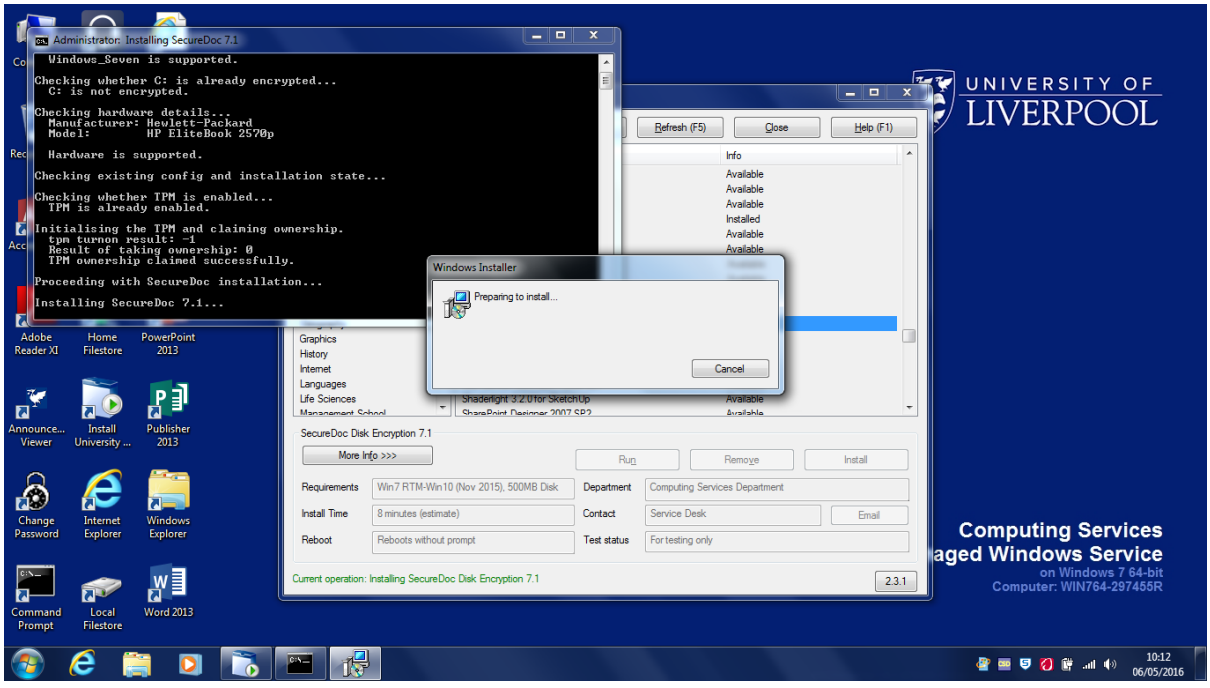
Assuming your computer is supported hardware and no existing encryption has been applied, the installation will proceed.

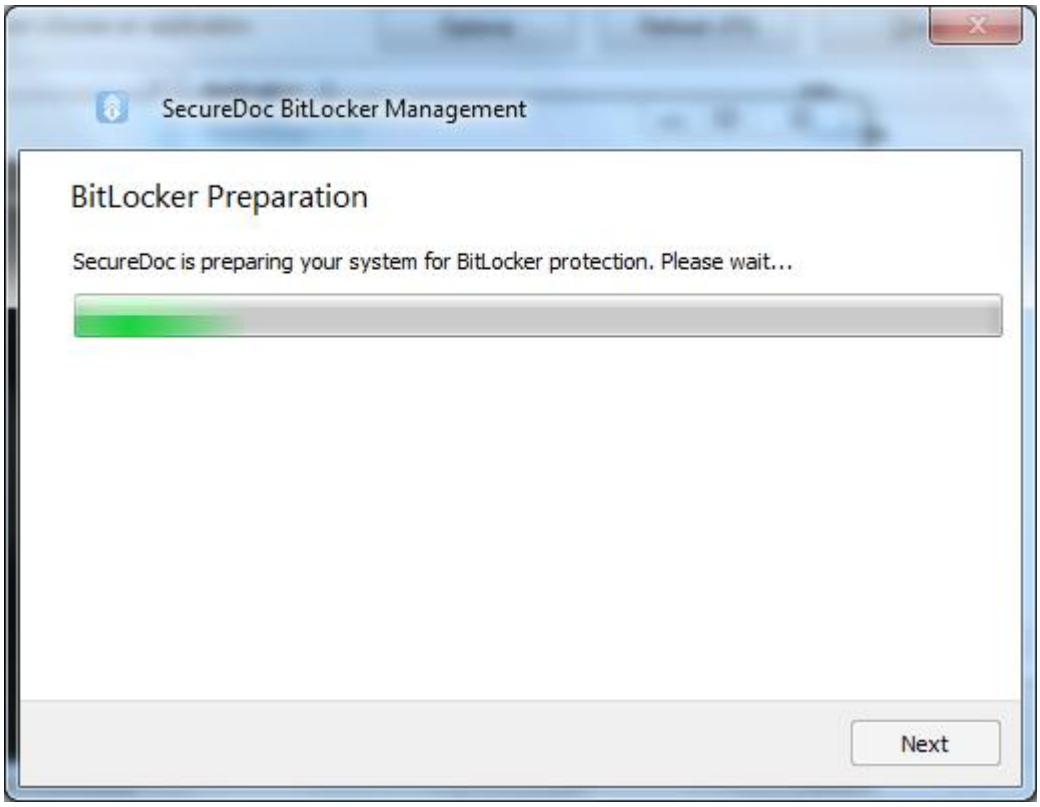


- Press any key to continue – the machine will **reboot** at this point.

- Once the computer has restarted, log on again, and run the same entry (**SecureDoc**) from **Install University Applications**. SecureDoc will still show as “available” not “installed”, as the SecureDoc software itself has not been installed yet.

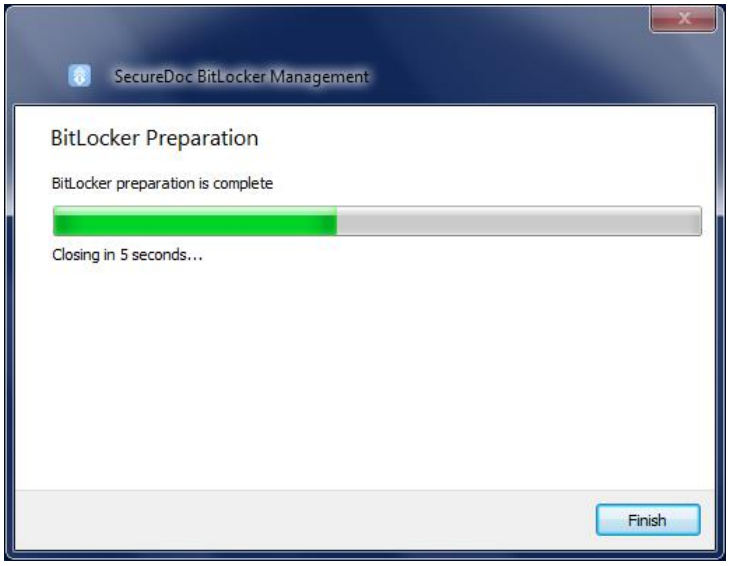
- On running the entry again, the installation process will complete the same checks again but this time proceed with the remaining steps and install the SecureDoc software.

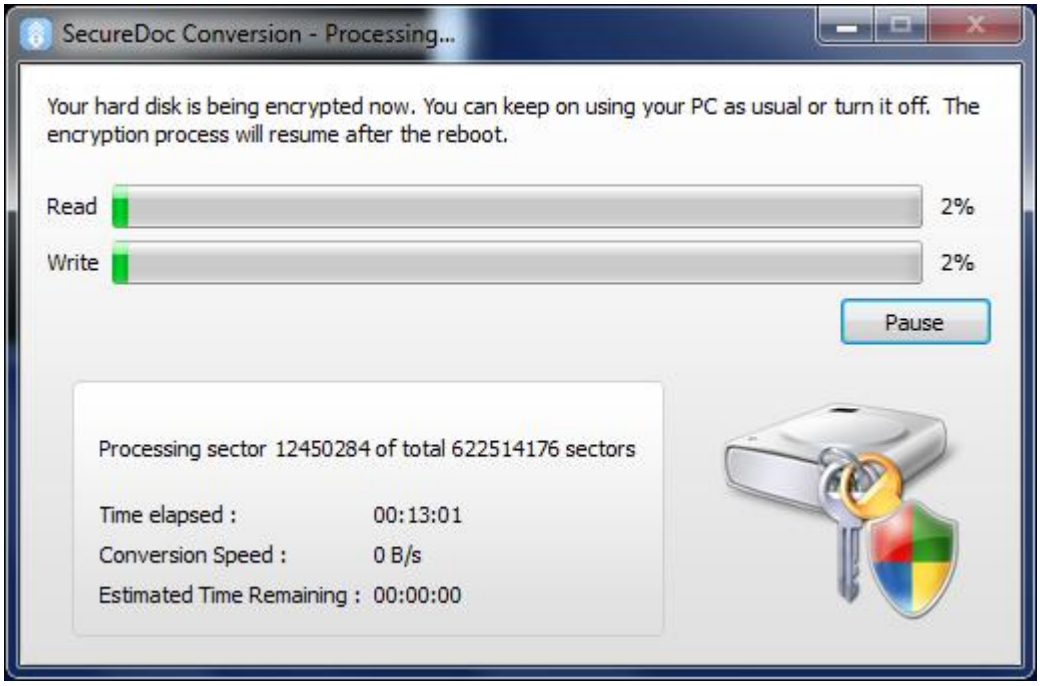




- SecureDoc will then reboot the PC without prompting.

- Log on again. SecureDoc will start the encryption process automatically. You will see a progress indicator. Note that the speed and time remaining indicators can take some time to appear properly.





- Once the encryption has started, it will continue in the background no matter what – yiu can reboot, etc and encryption will continue when you restart your computer until its completion.

The length of time is takes to encrypt the computer will vary greatly, depending on disk technology (traditional HD vs SSD), operating system and either disk size or amount of data present.

It can take anything from 15 minutes through to several hours.

On machines where encryption is complete, the pre-login MWS wallpaper will update to add the text “Encrypted with BitLocker” below the computer name. This happens on the first login after encryption has completed, and so is not visible until logging off afterwards.

Other notes:

The error messages for unsupported hardware and existing encryption are covered previously.

Other factors may also result in an error and a message to contact the Service Desk:

- Unsupported Operating System - currently the encryption only works with Windows 7 and Windows 10. Windows 8/8.1 is not supported. Machines with Windows 8 or 8.1 should move to Windows 10 before being encrypted.
- Unable to read TPM status – please register to attend one of the drop-in support clinics if you see this message. It means that either there is no TPM chip present at all, or BIOS options have been set to completely disable it and hide it from the OS. The TPM chip needs to be available for encryption to be installed.
- Attempting to initialise the TPM returned an error – please register to attend one of the drop-in support clinics.

Full contact details for the CSD Service Desk are available on the CSD website by visiting: http://www.liverpool.ac.uk/csd/getting-help/