UNIVERSITY OF WOLVERHAMPTON
KNOWLEDGE ▪ INNOVATION ▪ ENTERPRISE

16/17

BitLocker Encryption – User Guide

This document provides guidance for users of the BitLocker Encryption software installed on University of Wolverhampton managed staff devices as part of the Information Security Project 2016/17 rollout.

Further guidance and assistance can be obtained by contacting the ITS Service Desk (ext.2000).

UNIVERSITY OF WOLVERHAMPTON
KNOWLEDGE ▪ INNOVATION ▪ ENTERPRISE

TABLE OF CONTENTS

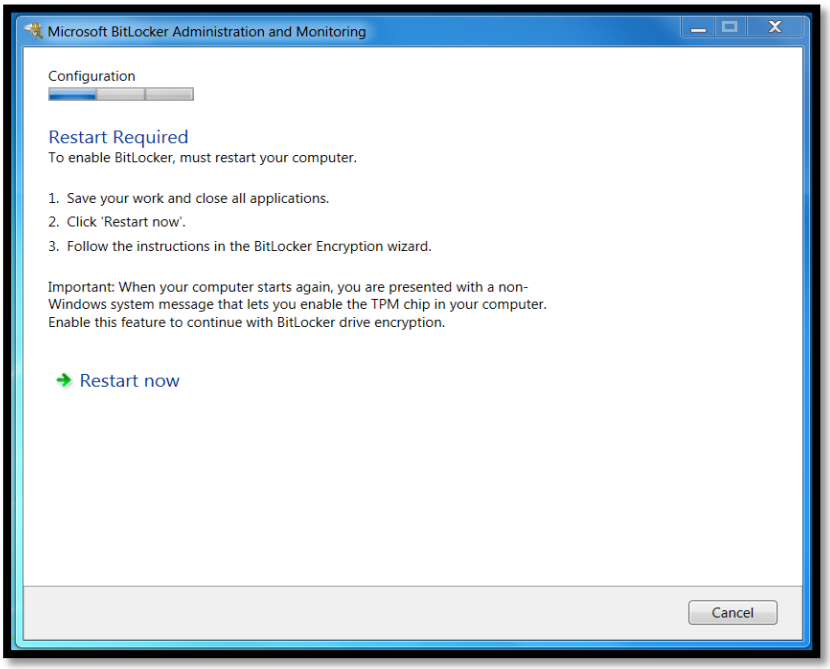
Authors: Steve Hill & Mita Patel

DESKTOP BITLOCKER ENCRYPTION – PROCESS

BitLocker hard drive encryption will be scheduled for activation on your device as part of a planned rollout to all staff laptops. The following screen will be displayed allowing the process to begin:

You can select the **Postpone** option to delay the encryption process, however after a period of 21 days have passed the Postpone button will deactivate and you will only have the option to start the process

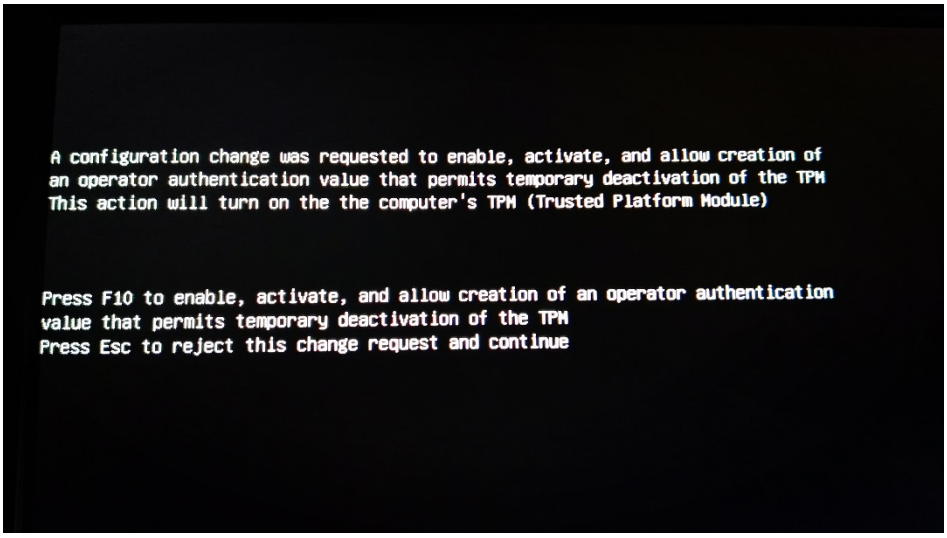
1) Select **Start** to commence the process and the following **Configuration – Restart Required** screen will be displayed



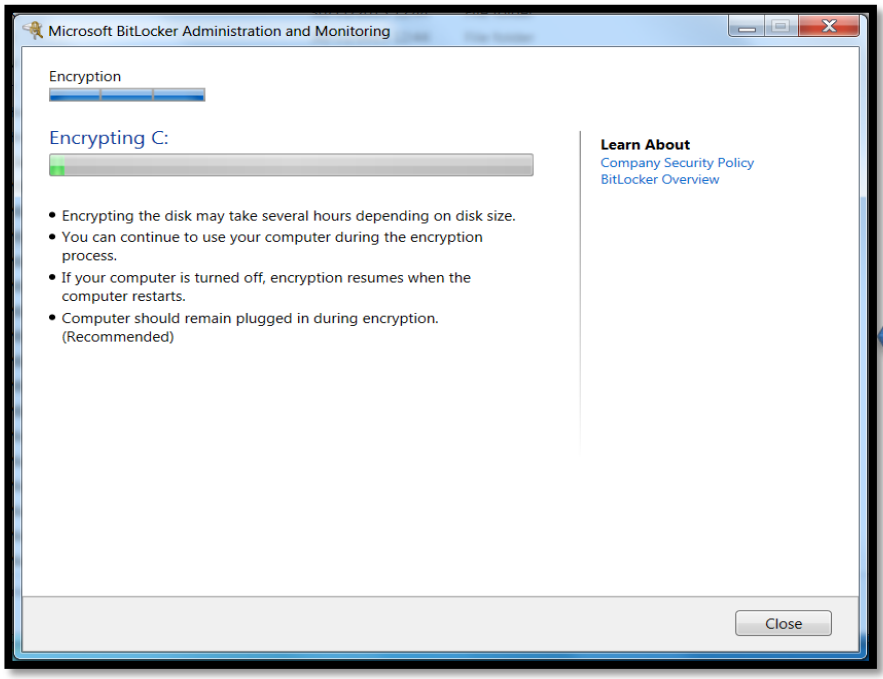
This screen tells you that when your computer is restarted you will need to enable a device change to allow BitLocker drive encryption process to continue

2) Select **Restart Now**

3) Upon a restart you **may** be presented with a similar screen to one show below, follow the instructions provided on the screen to continue the process of encrypting your device:



4) When you log back in the encryption process will have started for which you will be presented with the following screen:



YOU MAY

Close this window and the encryption process will continue in the background.

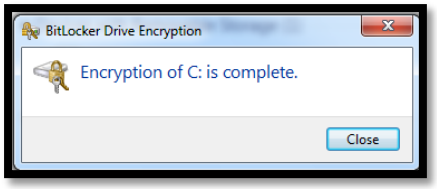
Continue using the device whilst encryption is taking place.

Shutdown and restart your device as required. The process will continue next time the device is

How long this takes is dependent on various factors including:

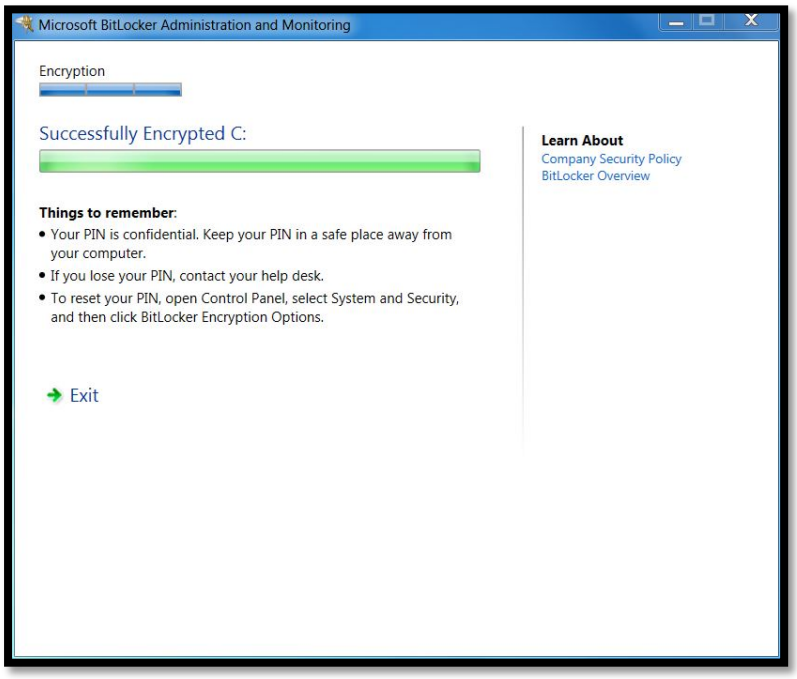
- The size of the hard drive
- The amount of data stored on the disk
- The age of the machine

5) You will see with one of the following prompts when the encryption process has successfully completed:



Click **Close**

OR



Click **Exit**

Authors: Steve Hill & Mita Patel

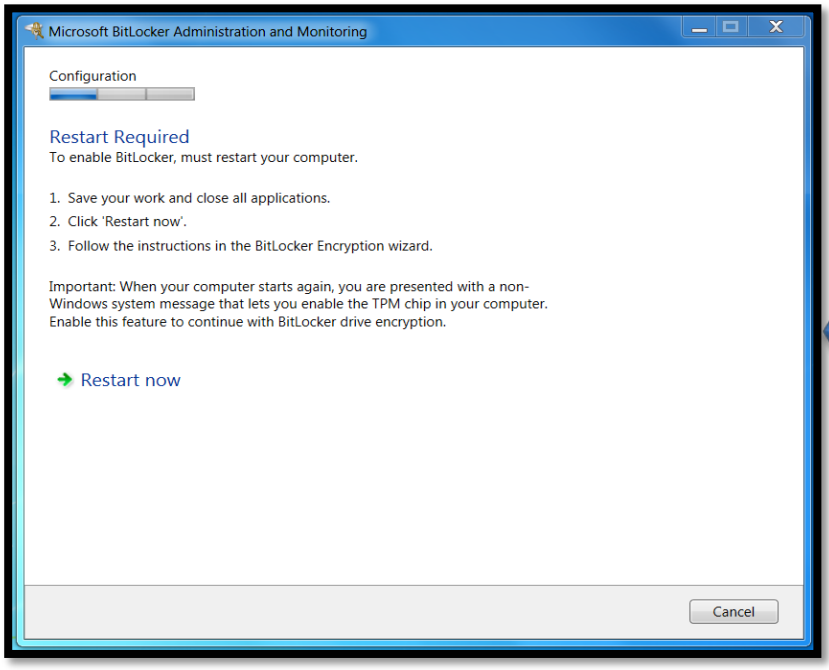
LAPTOP BITLOCKER ENCRYPTION – PROCESS

Ensure your laptop is connected via the mains power before continuing

BitLocker hard drive encryption will be scheduled for activation on your device as part of a planned rollout to all staff laptops. The following screen will be displayed allowing the process to begin and will appear every 90 minutes if postponed.

You can select the **Postpone** option to delay the encryption process, however after a period of 21 days have passed the Postpone button will deactivate and you will only have the option to start the process

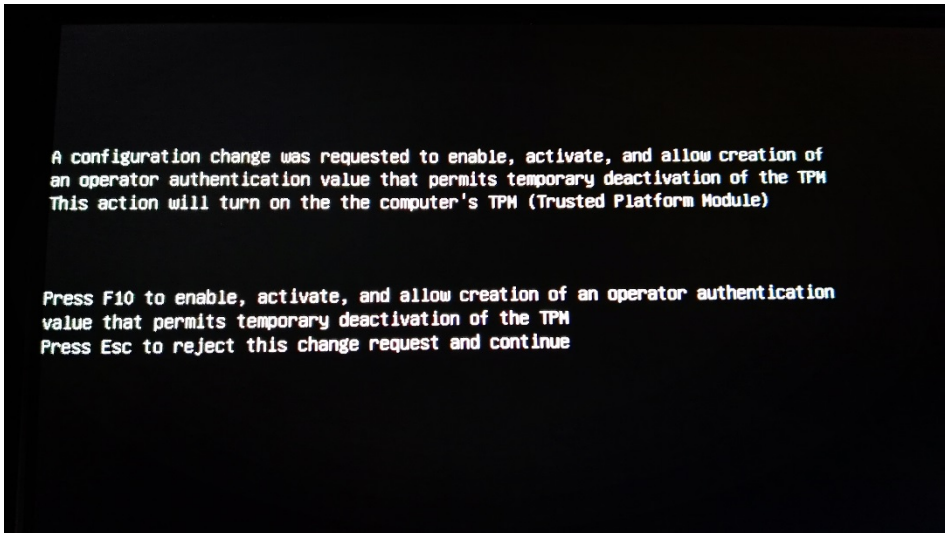
1) Select **Start** to commence the process and the following **Configuration – Restart Required** screen will be displayed



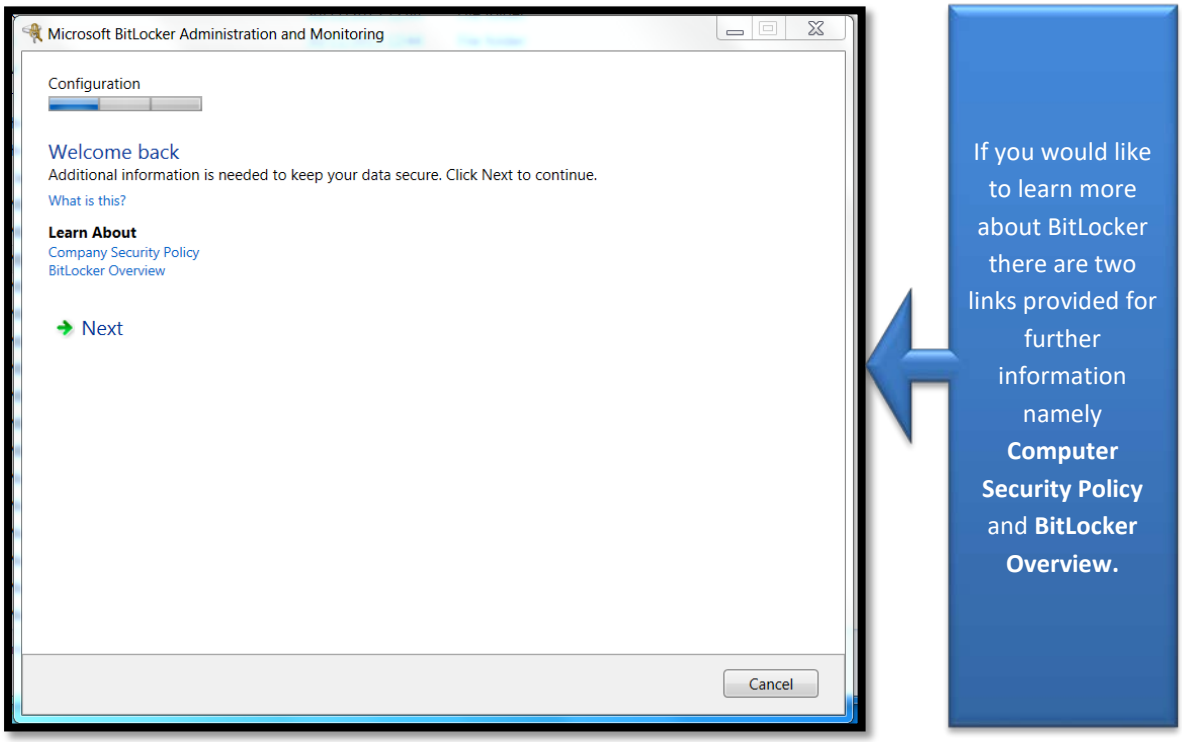
This screen tells you that when your computer is restarted you will need to enable a device change to allow BitLocker drive encryption process to continue

2) Select **Restart Now**

3) After your laptop restarts a screen similar to the following will be presented:

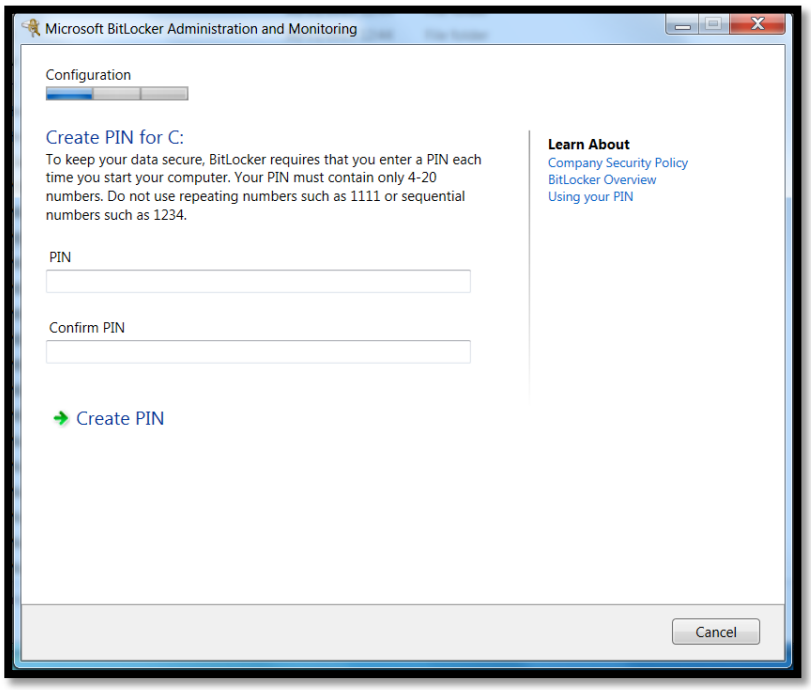


4) BitLocker is requesting permission to make the required configuration changes to your laptop, press **F10** to allow the changes to be made.
5) Your device will restart and load Windows, when it has done this log into your device as normal.
6) Once you have logged onto your laptop you will be prompted with the **Configuration – Welcome Back** screen:



7) Select **Next** to proceed

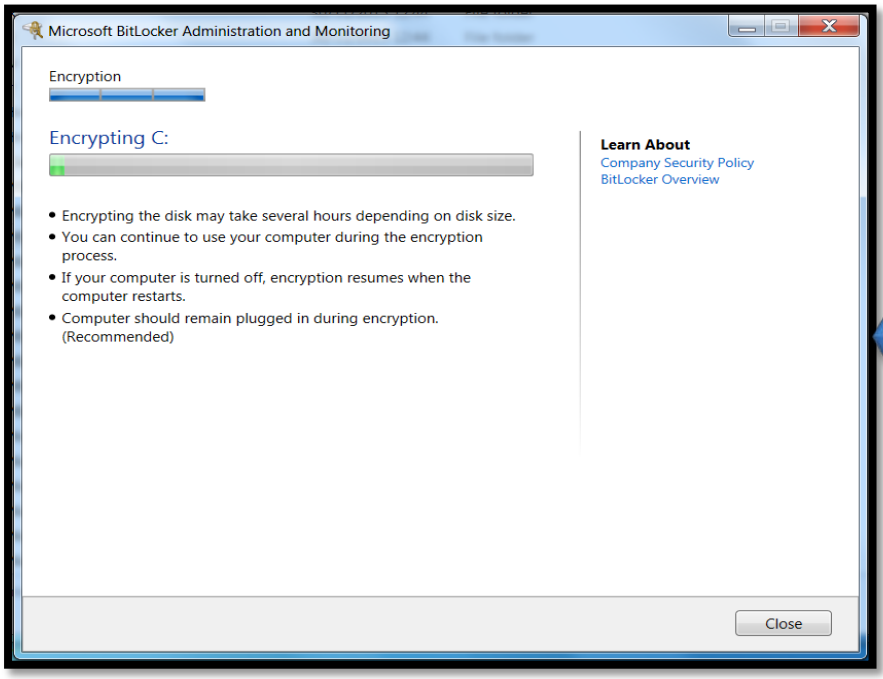
8) You will be presented with the following **Configuration – Create PIN for C:** screen:



This screen will guide you in creating a BitLocker PIN

9) Please enter a numeric 4-digit PIN in both fields
NOTE: repeating numbers such as 1111 or sequential numbers such as 1234 are **NOT** allowed

10) Click **Create PIN** and the encryption process will begin as per the following screenshot:



YOU MAY

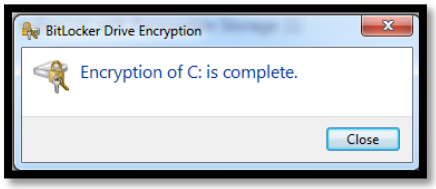
Close this window and the encryption process will continue in the background.

Continue using the device whilst encryption is taking place.

Shutdown and restart your device as required. The process will continue next time the device is

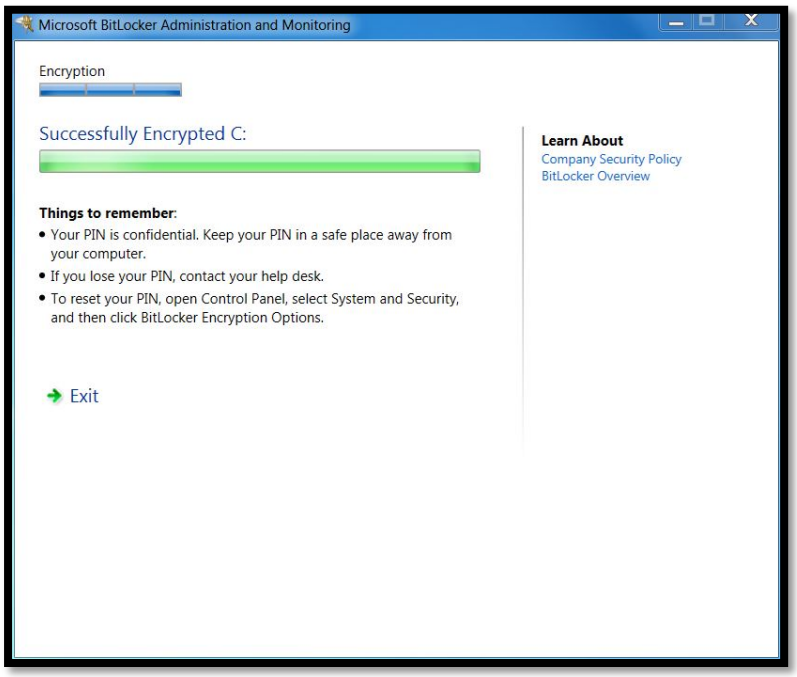
11) How long this takes is dependent on various factors including:
    - The size of the hard drive
    - The amount of data stored on the disk
    - The age of the machine

12) You will see with one of the following prompts when the encryption process has successfully completed:



Click **Close**

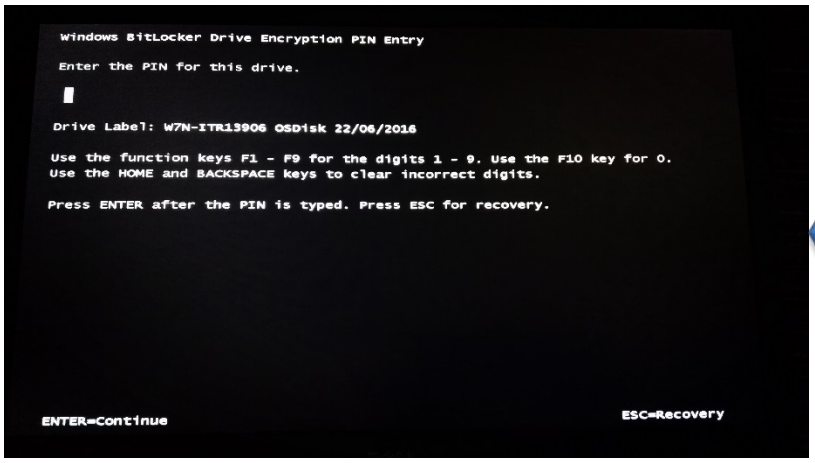
OR



Click **Exit**

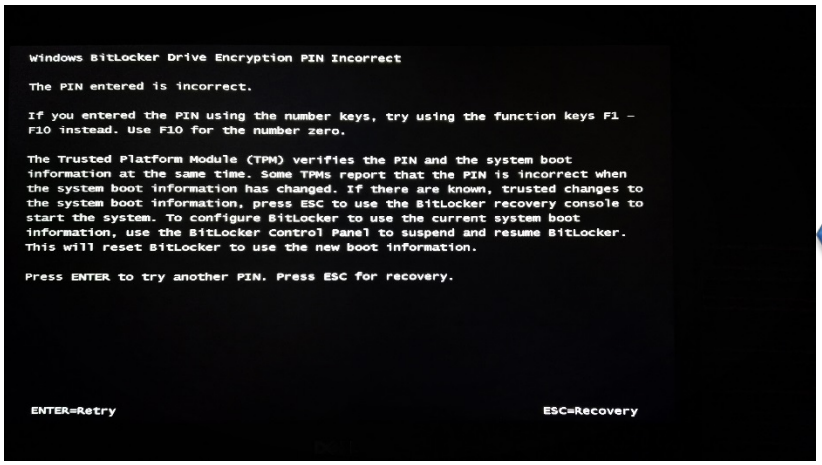
LAPTOP BITLOCKER ENCRYPTION - LOGON

Once your laptop has been encrypted, every time you power on you will be presented with the **Windows BitLocker Drive Encryption PIN Entry** screen, as shown here:



Enter your PIN to continue start-up of your device

If you input an incorrect PIN the laptop will display the **Windows BitLocker Drive Encryption PIN Incorrect** screen:



This screen is telling you that you have entered an incorrect PIN

Try again by pressing **Enter** or select **ESC** to go through to recovering your PIN

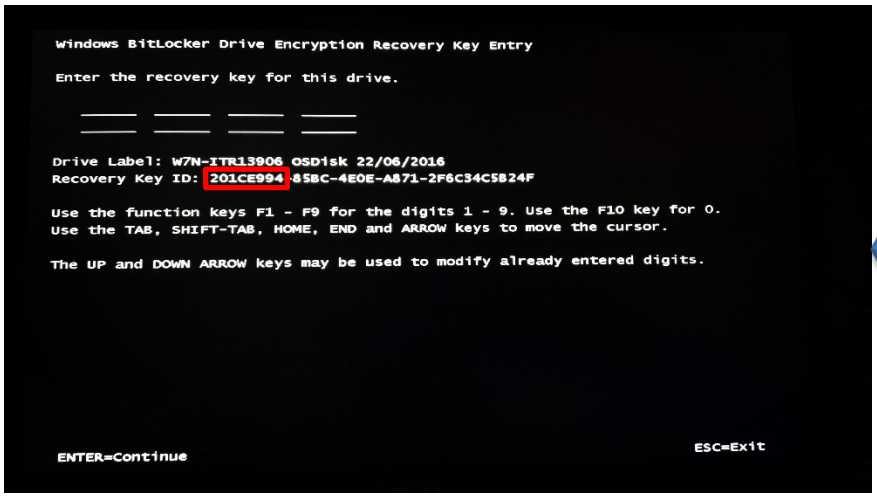
Authors: Steve Hill & Mita Patel

LAPTOP BITLOCKER ENCRYPTION - LOST / FORGOTTEN PIN

If you are unable to logon at this point don't worry, you will need to enter a **BitLocker Recovery Key** which you can obtain in one of the following ways:

- By accessing the BitLocker Self-Service Portal, if you have another device available to access
- By contacting the ITS Service Desk

You will be presented with the **Windows BitLocker Drive Encryption Recovery Key Entry** screen:



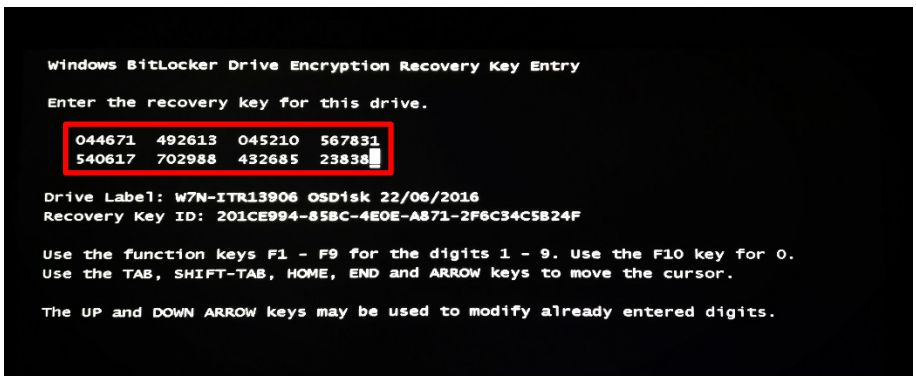
You will need to give the first 8-digits of Recovery Key ID when you contact the ITS Service Desk or the BitLocker Self-Service portal

CONTACTING THE ITS SERVICE DESK

When you contact the ITS Service Desk requesting a recovery key for your laptop they will ask you for the following:

- Your username
- The first 8-digits of your recovery key ID (as per screenshot above)

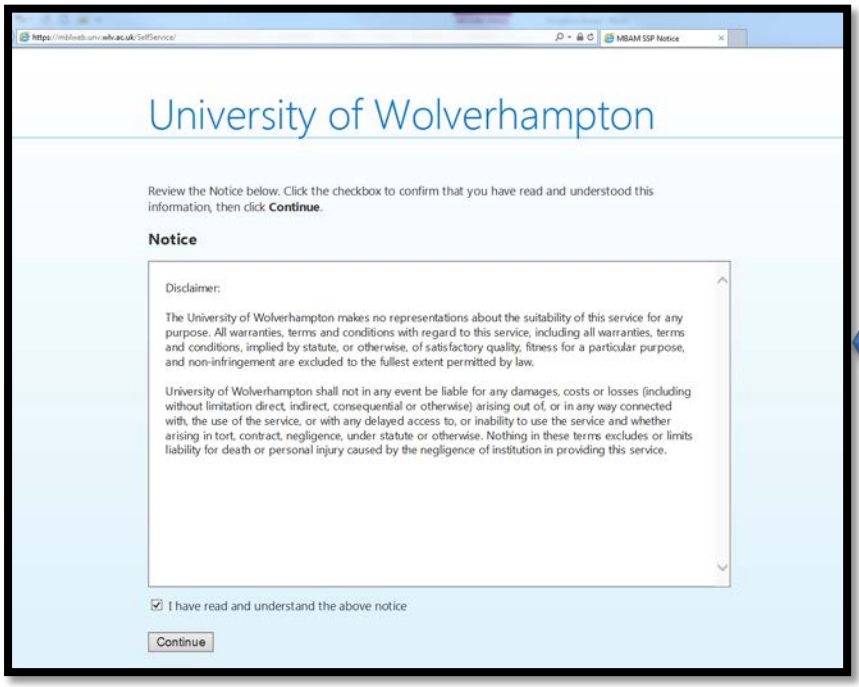
They will give you a 48-digit code which you will need to enter as per below:



ACCESS BITLOCKER SELF-SERVICE PORTAL

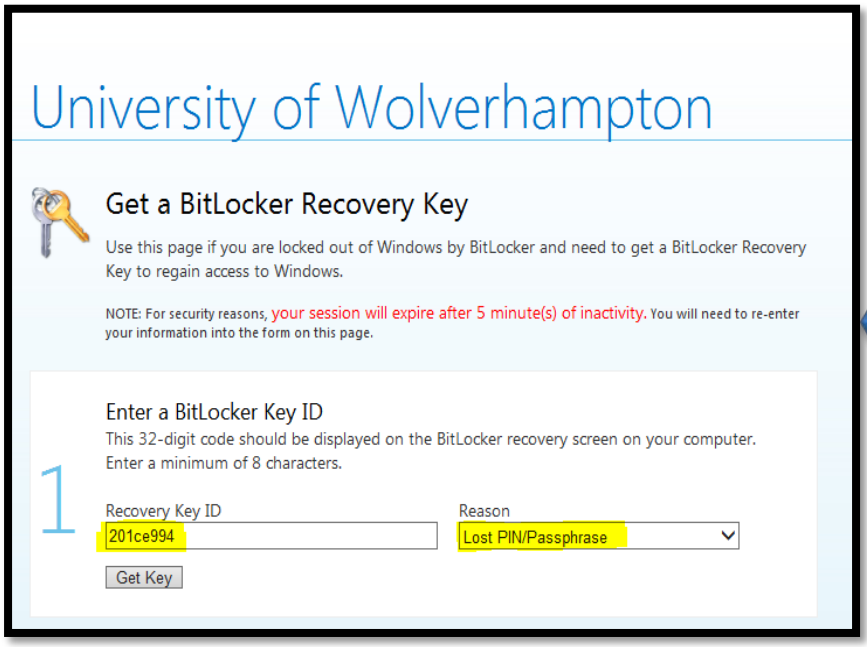
If you have forgotten your PIN and have access to another device with a web browser, you can use the Self-Service Portal at https://mblweb.unv.wlv.ac.uk/SelfService to get a recover key which will enable you to access your laptop.

The Self-Service Portal can be accessed both on and off-campus via a Web browser.



Select **I have read and understand the above notice** and select **Continue**

1) You will then be displayed with the Get a BitLocker Recovery Key page:

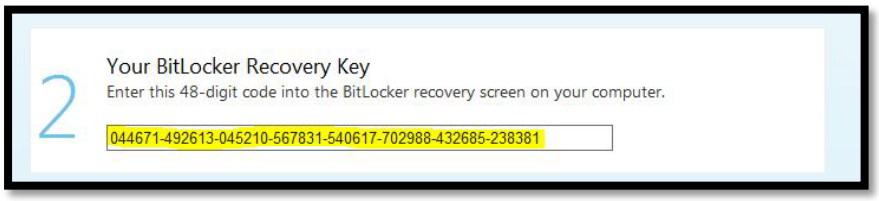


Enter the first eight digits of the **Recovery Key ID** from the device you are accessing.

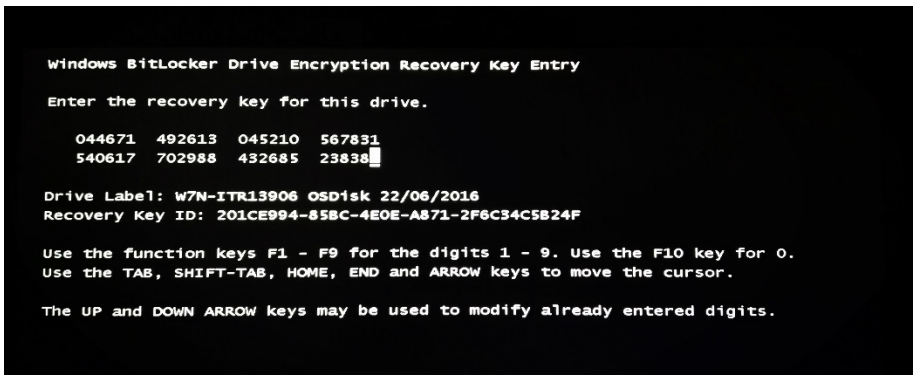
Select a **Reason**

Select **Get Key**

2) This will create your 48-digit BitLocker Recovery Key.



3) Enter this code into your device at the BitLocker Drive Encryption Recovery Key Entry screen:



4) When you have entered the last digit of the code your device will continue to boot into Windows.

REMEMBER..!

Now you have regained access to your device you should reset your PIN before restarting or shutting down.

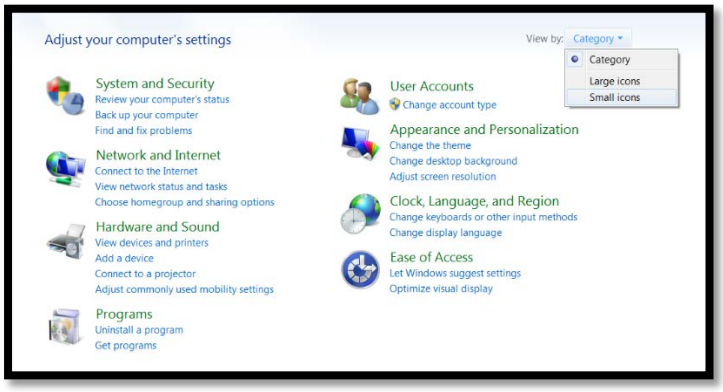
Please go to the BitLocker PIN Reset section of this document

BITLOCKER PIN RESET

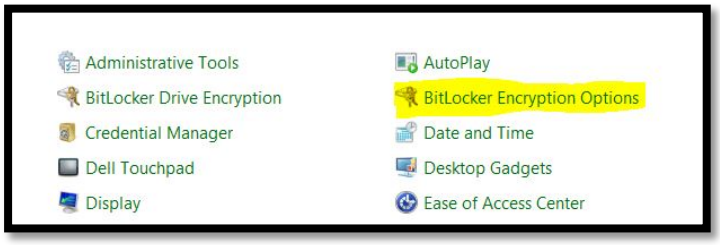
Resetting your PIN is a simple process with only two steps required on your laptop:

1) Upon successful log onto your laptop, open Control Panel by selecting **Start** > **Control Panel:**

2) Change the view of your control panel to **small icons** if required:

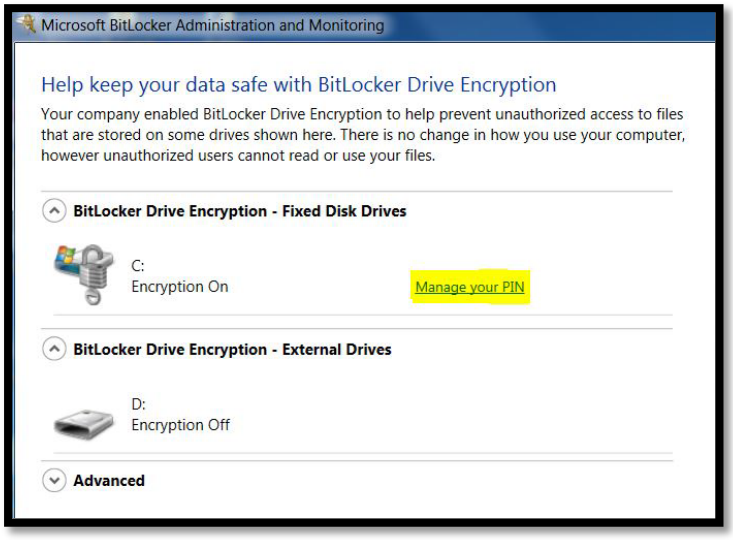


3) Select **BitLocker Encryption Options.**

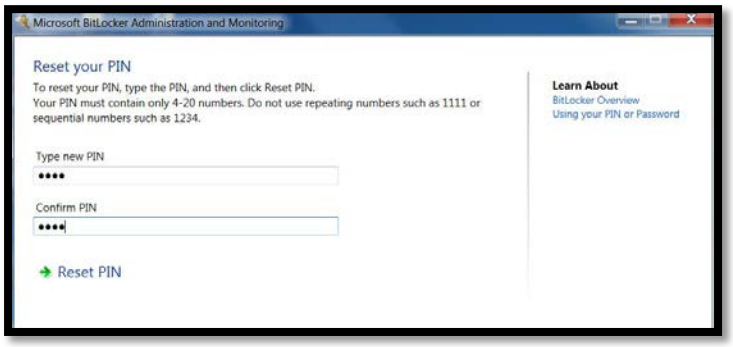


Authors: Steve Hill & Mita Patel

4) You will see the following screen, select **Manage your PIN.**



5) At the Reset Your PIN screen, enter a new PIN in both fields provided and select **Reset PIN.**



6) Your PIN has now been reset and you will be prompted for this new PIN next time your device is restarted.

SHARED LAPTOP BITLOCKER ENCRYPTION PROCESS

Shared laptops will follow similar steps to Desktop encryption, users will be prompted to encrypt the device by following the on-screen instructions.

If a shared laptop has already been setup with a PIN from previous methods of encryption the device would need to be re-imaged to allow encryption without a PIN.

PLEASE NOTE: Users are reminded that in no circumstances should personal or commercial sensitive data be stored on shared laptops. Storage of such data on shared devices is a breach of University policy.