BitLocker Setup

A Step by Step Guide

Drive Preparation

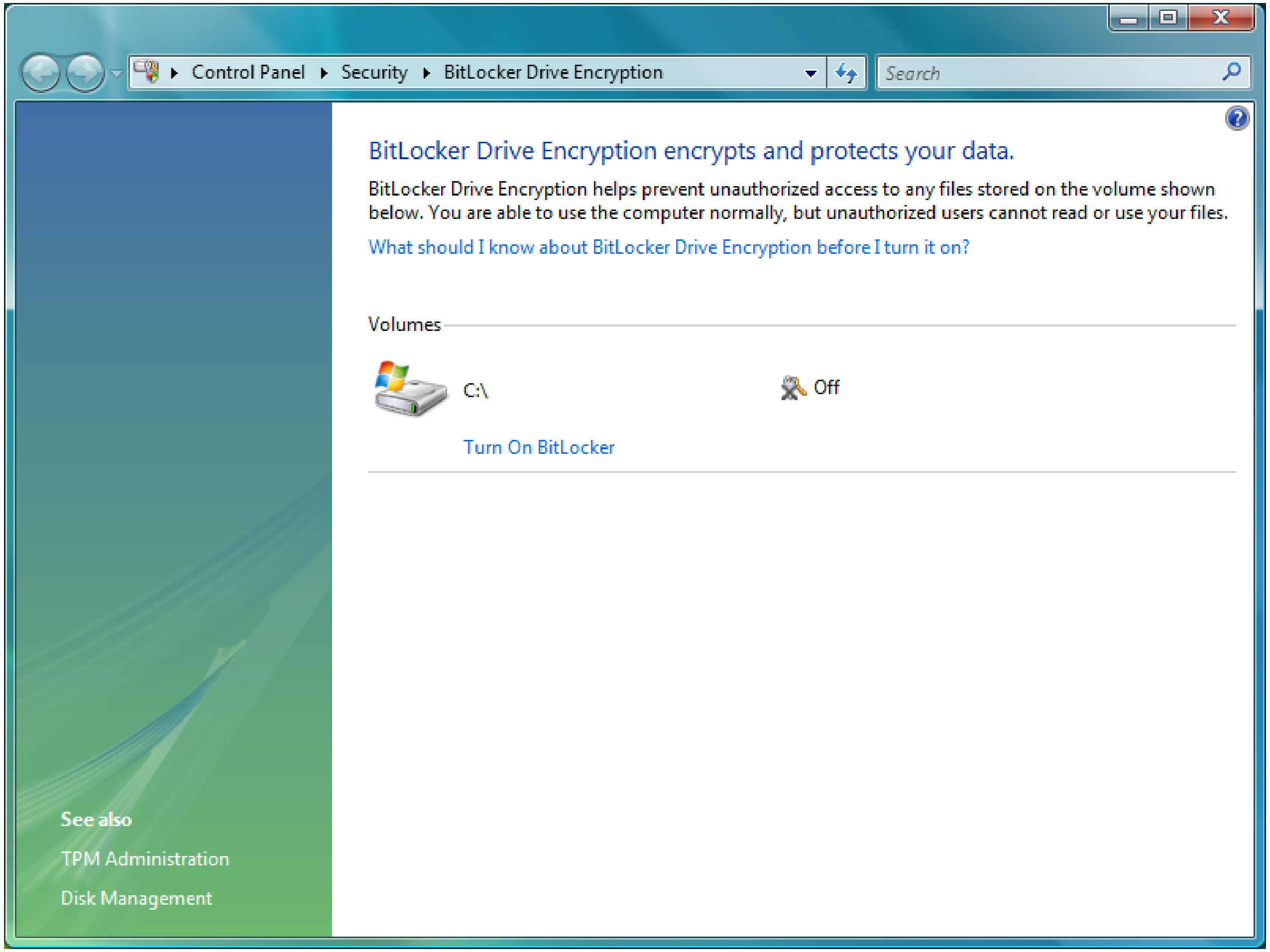
- For BitLocker to work you need two volumes on your hard drive
- One for the Windows start files which won’t be encrypted (about 5Gb)
- One for all the other files
- You can use a Microsoft downloadable tool to do this for you

Download

Run BitLocker

- After running the drive preparation tool and restarting your PC / Laptop you can start the BitLocker process
- The next few slides show you the process

Turn BitLocker On



BitLocker Drive Encryption encrypts and protects your data.

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the volume shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.

What should I know about BitLocker Drive Encryption before I turn it on?

Volumes

C:\ Off

Turn On BitLocker

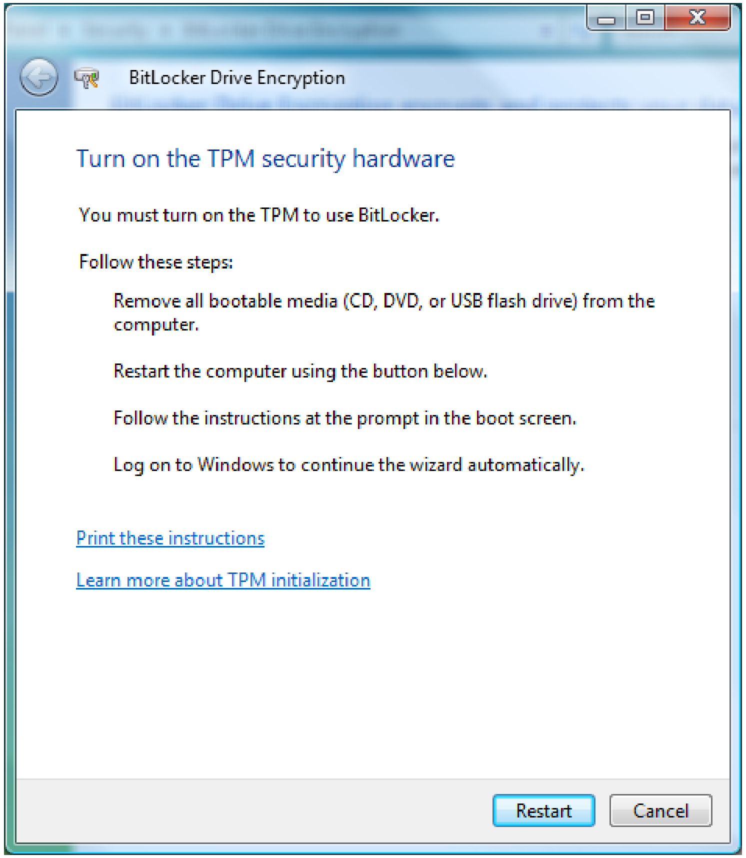
See also

TPM Administration

Disk Management

TPM Security

- If you have a fairly new machine it may have a TPM chip installed
- The 'Trusted Platform Module' is used to generate cryptographic keys
- If you want to learn more about TPM then you can look it up on Wikipedia



Turn on the TPM security hardware

You must turn on the TPM to use BitLocker.

Follow these steps:

Remove all bootable media (CD, DVD, or USB flash drive) from the computer.

Restart the computer using the button below.

Follow the instructions at the prompt in the boot screen.

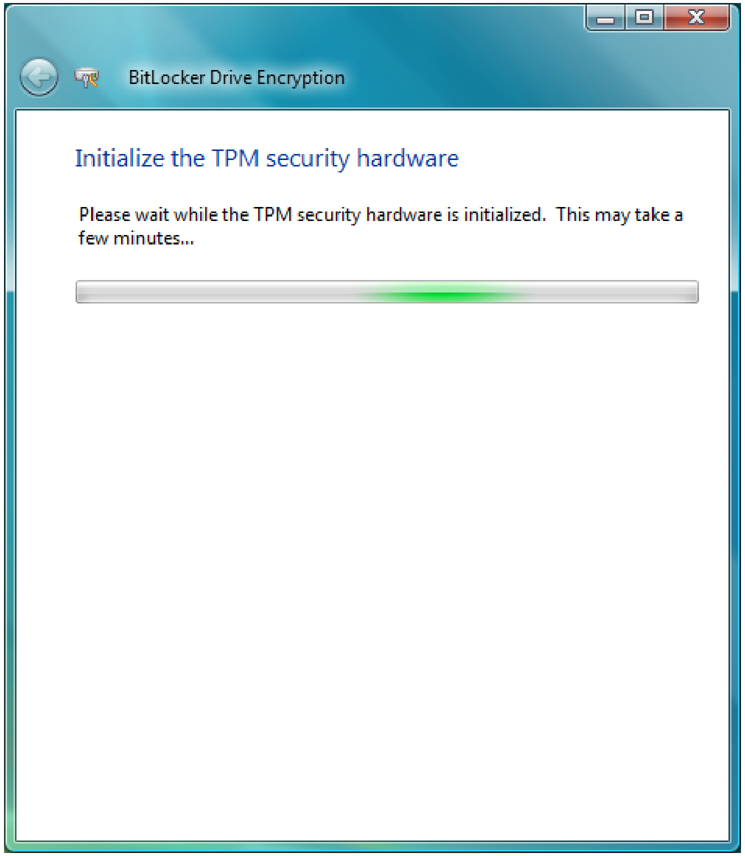
Log on to Windows to continue the wizard automatically.

Print these instructions

Learn more about TPM initialization

TPM Security

- Once you have restarted your machine the TPM chip will initialise and then we can continue with BitLocker



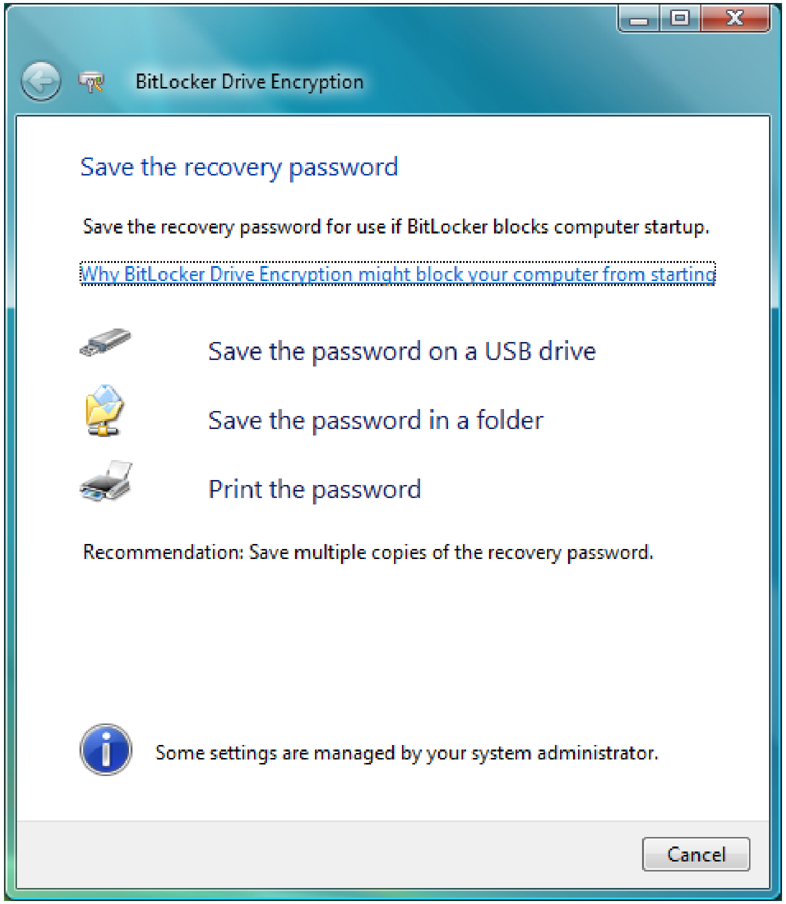
Initialize the TPM security hardware

Please wait while the TPM security hardware is initialized. This may take a few minutes...

Recovery Password

- Save multiple copies of the recovery password

- USB
- Print it
- Save it on a network drive



Save the recovery password

Save the recovery password for use if BitLocker blocks computer startup.

Why BitLocker Drive Encryption might block your computer from starting

Save the password on a USB drive

Save the password in a folder

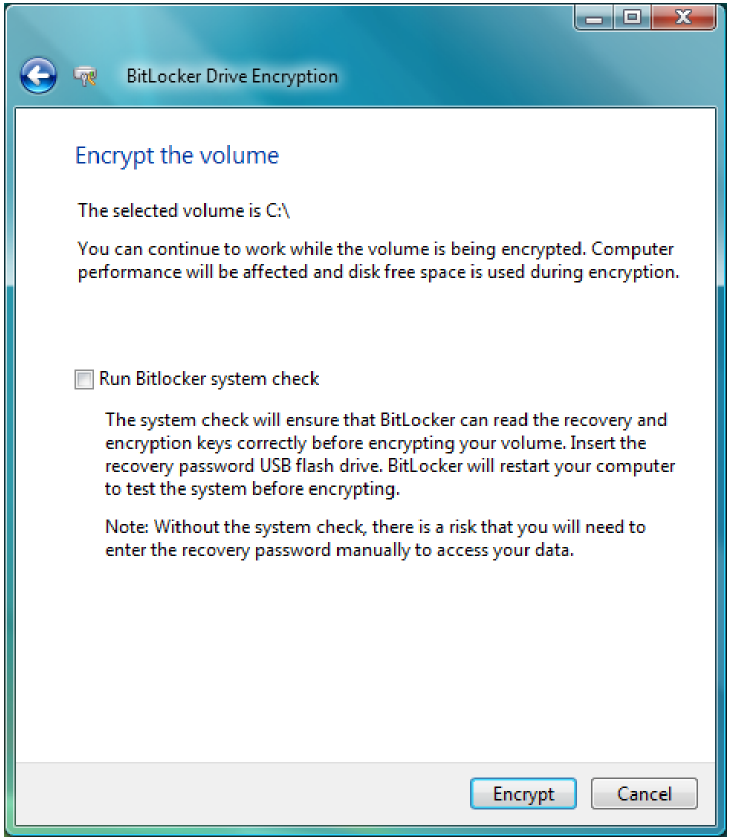
Print the password

Recommendation: Save multiple copies of the recovery password.

Some settings are managed by your system administrator.

Encrypt

- The next phase is the actual encryption
- If you want to you can run a system check before encryption



Encrypt the volume

The selected volume is C:\

You can continue to work while the volume is being encrypted. Computer performance will be affected and disk free space is used during encryption.

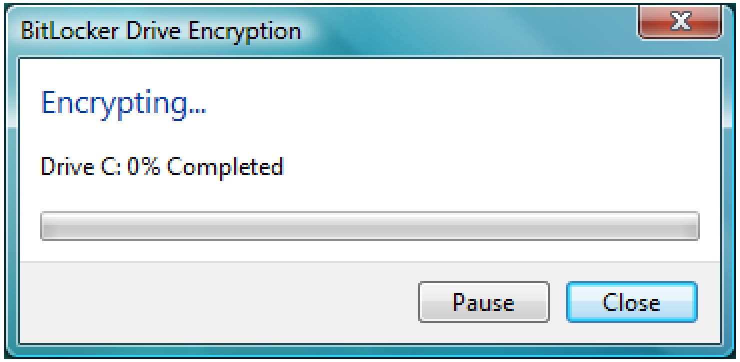
□ Run Bitlocker system check

The system check will ensure that BitLocker can read the recovery and encryption keys correctly before encrypting your volume. Insert the recovery password USB flash drive. BitLocker will restart your computer to test the system before encrypting.

Note: Without the system check, there is a risk that you will need to enter the recovery password manually to access your data.

Encrypting

- Your drive is now being encrypted
- This can take a while but you can carry on working while it is doing it, although your machine will be slow
- Don’t worry about the free space that suddenly disappears on your hard drive, this will come back once encryption is complete



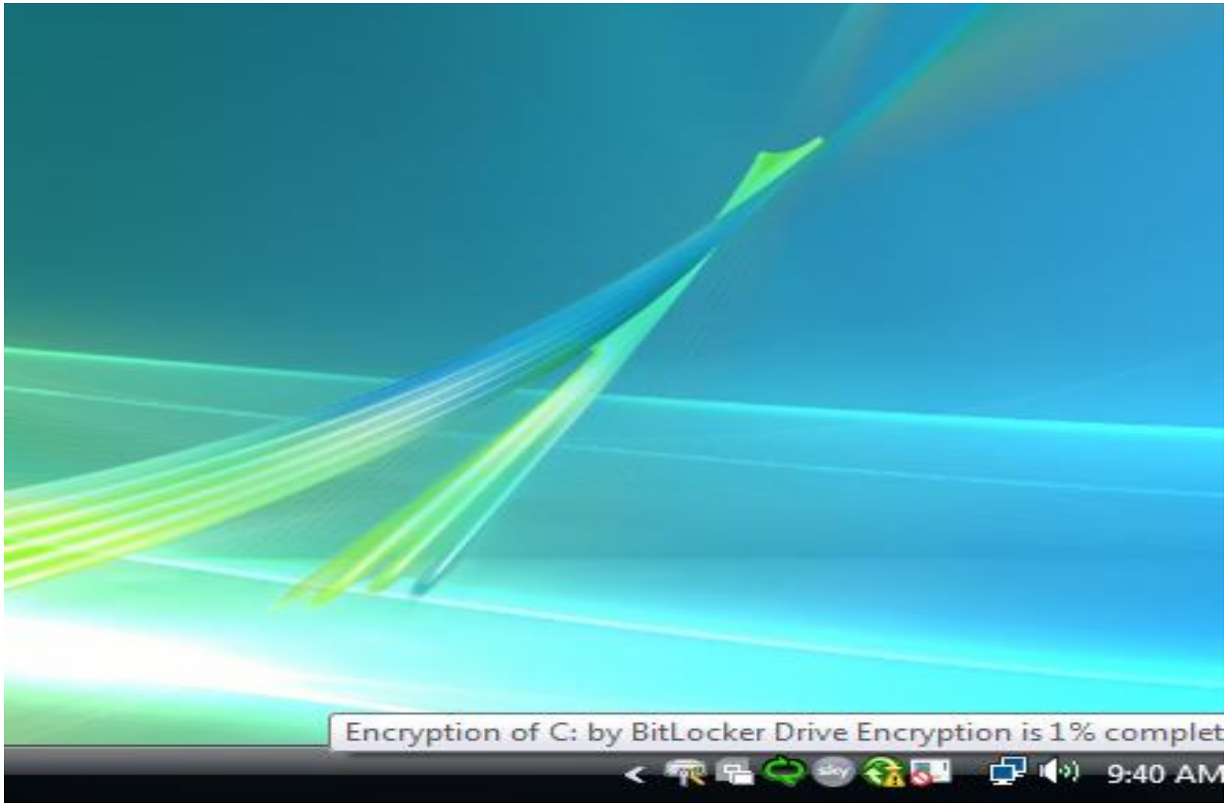
BitLocker Drive Encryption

Encrypting...

Drive C: 0% Completed

Encrypting

- Encryption is ongoing while you work



Encryption of C: by BitLocker Drive Encryption is 1% complet