How To Encrypt a Windows 7, 8.1 or 10 laptop or tablet

Introduction

College sensitive information stored on a mobile computing device is at risk for unauthorized access and disclosure if appropriate security measures are not implemented to protect the device against loss or theft of information.

The best way to protect College sensitive information is to not store it on a mobile computing device; however, it is recognized that storage of College sensitive information on a mobile computing device may be necessary in certain situations. In these cases, encryption provides protection against unauthorized access and disclosure.

This article provides instructions for using Microsoft's Bitlocker encryption technology to encrypt and protect data stored on Windows laptops or tablets. (BitLocker is a security mechanism that provides two primary functions: verification of the overall integrity of the Windows operating system at startup, and full-drive data encryption. Once BitLocker is enabled and configured, the file system on the protected drive(s) is unlocked, and the drive encryption does not interfere with running applications.)

Encryption must be used in concert with other security measures to maximize protection of information technology resources and of College sensitive information. Lethbridge College Information Technology has provided a Mobile Computing Security website that contains further information about other security measures.

Applicability

This article is intended for use by any faculty, staff, or student member who would like to safeguard data stored on a Windows laptop or tablet.

Note: Since Lethbridge College's most widely-deployed version of Windows is Windows 7, this article will focus on setting up Bitlocker on that operating system. Relevant links to the Windows 8.1 and Windows 10 versions of these procedures are linked where needed.

Procedure

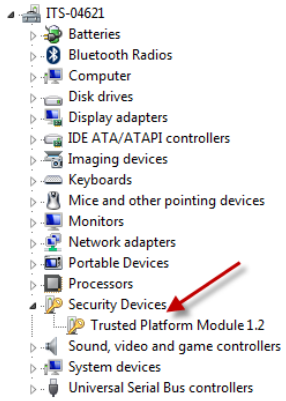
Prerequisites

Enabling BitLocker requires that the laptop has the correct hardware for storing a Master Volume Key (MVK) and related data. Microsoft allows this data to be stored in either a Trusted Platform Module (TPM) or on a USB drive. The College advises that BitLocker be enabled only on hardware with a functional TPM. Our experience is that USB drives are too easy to lose or damage when used in this context. Please note, if you do use a USB drive to backup your MVK contrary to this warning, and it becomes lost

or stolen, data recovery will not be possible. Your data will become encrypted and locked forever, and should be considered “securely destroyed”.

To check if your laptop has the necessary TPM module, perform the following steps:

1. **Windows 7**: Click **Start**. Right-click on **Computer**, then left-click on **Manage**. You may need to allow Administrator access.
2. **Windows 8.1**: Swipe in from the right edge of the screen, and then tap **Search**. Type *Device Manager* in the search box, and tap or click **Device Manager**. You may need to allow Administrator access. In the list of installed devices, look for: Trusted Platform Module (TPM)
3. **Windows 10**: Click **Start.** Type *Device Manager* in the search box and tap **Device Manage**r on the menu**.** You may need to allow Administrator access. In the list of installed devices, look for: Trusted Platform Module (TPM)
4. Click **Security Devices.**

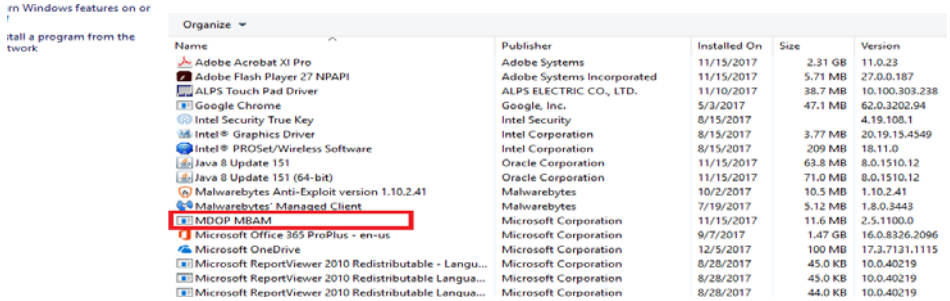


If there is no "Security Devices" option, or if there is no TPM listed, you may need to verify with the manufacturer to determine if TPM was an included option. If it was not, please contact the Help Desk at 403-320-3202 for further encryption options and assistance.

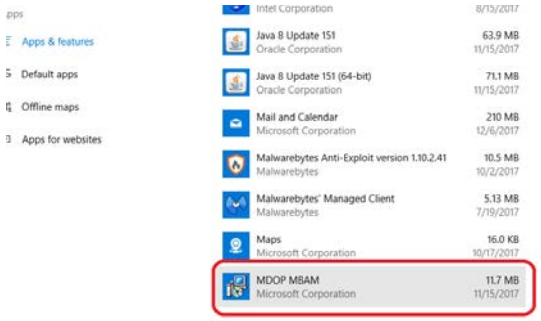
If you have a domain Windows laptop, your computer should have the Microsoft Bitlocker Administration and Management client. (MDOP MBAM).

The following instructions will guide you to discover if the client is installed.

1. For Windows 7: Click **Start.** Click **Control Panel.** Click **Programs and Features**. In the list of programs, you should see **MDOP MBAM** in the list of installed programs.



2. For Windows 10: Click **O** next to the **Start** menu. Type **Programs.** Click on **Add or remove programs.** You should see **MDOP MBAM** in the list of installed programs.



General instructions

Note: If at any time you have difficulty or encounter problems with this process, please contact the HelpDesk at 403-320-3202 or helpdesk@lethbridgecollege.ca.

Note: The instructions and screen captures presented here are primarily for Windows 7 computers, but the encryption process is essentially the same for Windows 8.1 and Windows 10. Some images and text may not exactly match your computer.

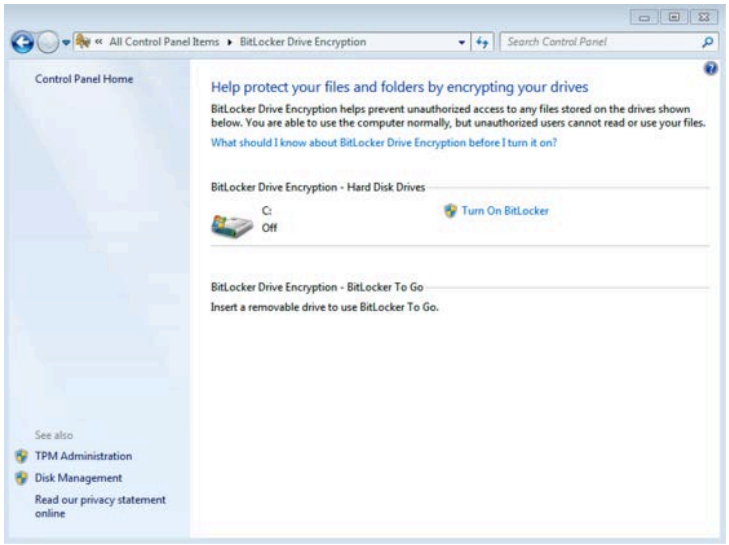
1. Follow the relevant steps for your device:

Windows 7: Click **Start**, click **Control Panel**, and then double-click **BitLocker Drive Encryption.**

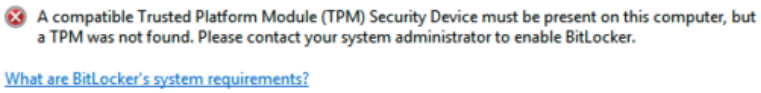
Windows 8.1: Click **Start**, click **Control Panel**, and select **System & Security BitLocker Drive Encryption.**

Windows 10: Open **File Explorer** and go to **This PC**. Right-click on **Local Disk (C:).**

2. Click **Turn On BitLocker** for the drive that you want to encrypt.

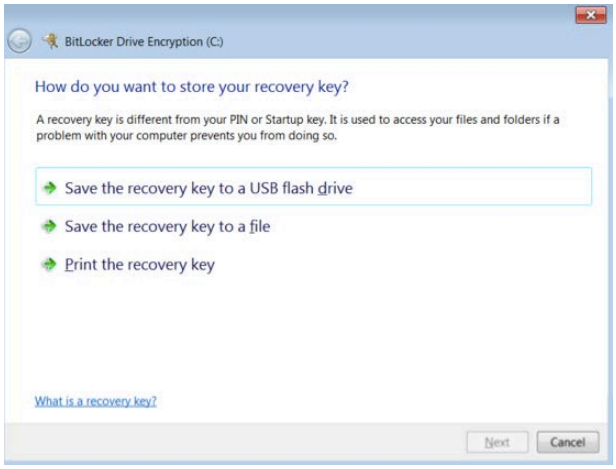


If you see the following warning, please stop the process and call the HelpDesk at 403.320.3202 for further encryption options and assistance.



3. On some versions of Windows, you will be prompted to create a BitLocker password. If you already log in to your computer using a password, you will likely not see this prompt.

4. The BitLocker setup wizard will ask you to choose how to store the recovery key.



You can choose from the following options:

1. Save the recovery key to a USB flash drive. (However, if you are trying to encrypt a USB drive, this option will not work.)
2. Save the recovery key to a file. (This saves the recovery key to a network drive or other location, such as a recovery partition on your hard drive, or USB removable drive. However, you cannot save the encryption recovery key to the same hard drive you're trying to encrypt.)
3. Print the recovery key. You may print to a regular printer or a PDF but if you store this document on the encrypted device, you may lose this information in the event you are locked out of the device.

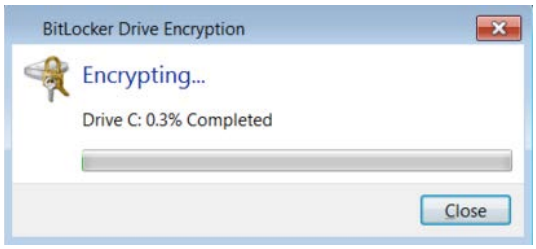
Use one or more of these options to preserve the recovery key. Click **Save** to store your recovery key.

For maximum security, you should store recovery keys apart from the drives they are associated with.

5. The BitLocker setup wizard will ask if you are ready to encrypt the drive.

- **Windows 7:** Click **Start Encrypting**
- **Windows 8.1 and 10**: You will be prompted to reboot the computer, and will then be asked to supply your Bitlocker password. After this, click **Continue**.

The "Encrypting..." status bar will be displayed. You can monitor the ongoing status of the drive encryption by moving the mouse pointer over the BitLocker Drive Encryption icon in the notification area, at the far right of the taskbar, near the clock.



6. When encryption is complete, you may be prompted to restart your computer again to finalize the process.

Backup Considerations

The encryption provided by BitLocker is transparent to applications on the running operating system, and existing backup schemes should not require technical accommodations to be effective, provided the backup is server-based. Backing up a BitLocker protected system to unencrypted removable media, such as a USB drive, is strongly discouraged as it leaves the data mobile while simultaneously removing any benefit of protection provided by the encryption.

Data Recovery

Microsoft provides a number of data recovery methods. Their availability depends on the deployment scheme chosen. In the basic one-to-one scheme, where BitLocker is configured on each individual system, these recovery mechanisms are either a binary key or a long numeric passphrase.