# Lab - Bitlocker and Bitlocker To Go

## Introduction

Encryption can protect the data on your device by making it only accessed by people who have authorization. If device encryption is not available on your device, you might be able to turn on standard BitLocker encryption instead.

**Note**: BitLocker is only available on these Windows versions:

- Ultimate and Enterprise editions of Windows 7
- Pro and Enterprise editions of Windows 8 and 8.1
- Pro, Enterprise and Education editions of Windows 10

In this lab, you will enable BitLocker encryption on a removable data drive and on the computer system drive.

## Recommended Equipment

- PCs running Windows
- A removable USB storage drive

## Instructions

## Part 1: Use BitLocker to Go

In this part, you will use BitLocker to Go to encrypt a removable storage drive.

### Step 1: Encrypt the removable drive.

a. Insert removable drive, such as a USB drive into the computer.

b. BitLocker is off by default and must be turned on for each drive that needs encryption. To turn on and configure BitLocker navigate to **Control Panel** > in Small icons view, click **BitLocker Drive Encryption**.

c. Under **Removable data drives**, expand the list as needed. Select **Turn on BitLocker** for the desired removable drive.

d. In the **Choose how you want to unlock this drive** window, check the **Use a password to unlock the drive** and then enter a password. Click **Next** to continue.

e. In the **How do you want to back up your recovery key**, select either **Print** or **Save to a file** and then click **Next**.

f. In the **Choose how much of your drive to encrypt** window, select **Encrypt entire drive** and click **Next**.

g. If you are prompted with the **Choose which encryption mode to use** window, select **Compatible mode** and click **Next** to continue.

h. In the **Are you ready to encrypt this drive** window, click **Start encrypting**.

i. After a few minutes, the removable drive will be encrypted. It can now be removed.

### Step 2: Access the encrypted drive.

a. Insert the removable drive previously encrypted in the previous step into the USB port on the computer.

b. Navigate to the USB drive in **File Explorer** or **Windows Explorer** and open the USB drive. (If you are unable to open the USB drive, right-click the encrypted drive, click **Unlock Drive**.)

c. Click the **More options** button. Notice there is an option to enter the recovery key. If the password is forgotten, the saved or printed recovery key from the previous step can be used to unlock the drive.

Question:

Why is it important to save a BitLocker recovery key?

***Type your answers here.***

d. Enter the password to unlock the USB drive. Now you are able to access the content on the encrypted drive.

### Step 3: Decrypt the drive.

a. Navigate to the **Control Panel** > in Small icons view, click **BitLocker Drive Encryption**.

b. Select the encrypted removable drive. If the drive is locked, enter the password to unlock it. Click **Turn off BitLocker**.

c. Click **Turn off BitLocker** when the message notifying you that the decryption process could take some time. Note the warning message so you do not damage the content on the drive.

d. Click **Close** when the decryption process is done.

## Part 2: Encrypt the Operating System Drive

In this part of the lab, you will use BitLocker to encrypt the operating system drive.

### Step 1: Turn on BitLocker.

a. Return to **Control Panel > System and Security > BitLocker Drive Encryption** to turn on BitLocker for the operating system drive.

b. Under **Operating system drive**, select **Turn on BitLocker**.

**Note**: If an error message appears stating the device cannot use a Trusted Platform Module, some additional steps must be taken to allow additional authentication at startup. Click **Cancel** and perform these additional steps:

1) Type **gpedit.msc** in the **Windows search** to open the **Local Group Policy Editor**.

2) Expand **Administrative Templates** in the left pane and click **Windows Components**.

3) In the Windows Components list, select **BitLocker Drive Encryption**. Select **Operating System Drives**. Select **Require additional authentication at startup**.

4) Inside the **Require additional authentication** at startup window, select the **Enabled** button, then click **Apply** and **OK** to close the window.

5) Close **Local Group Policy Editor** to return to the **BitLocker Drive Encryption** window and click **Turn on BitLocker**.

c. The **Choose how you want to unlock this drive** window will open. In this window check the **Use a password to unlock the drive** select **Enter a password** and then enter a password and click **Next**.

d. In the **How do you want to back up your recovery key** select either **Print** or **Save to a file** and then click **Next**.

e. In the **Choose how much of your drive to encrypt** window, select **Encrypt used disk space only** and click **Next**.

f. In the **Choose which encryption mode to use** window, select **New encryption mode** and click **Next**.

g. In the **Are you ready to encrypt this drive** window, make sure the **Run BitLocker system** check box is selected and click **Continue.** A message stating the computer must be restarted will appear.

h. Click **Restart now** to restart the computer.

i. When the computer restarts you will be prompted to enter your password to unlock the computer.

Question:

What is the function of a TPM in relation to BitLocker?

***Type your answers here.***

## Step 2: Turn off BitLocker.

a. To turn off BitLocker return to **Control Panel** > **System and Security** > **BitLocker Drive Encryption** to and select **Turn off BitLocker**.

b. Click **Turn off BitLocker to** decrypt the drive. This process may take a while depending on the size of the drive.