BitLocker To Go - For Portable USB Drives

BitLocker To Go - For Portable USB Drives

On this page:

Encrypt external storage drive

Important
BitLocker To Go is NOT an additional application you need to install. It is how BitLocker is referred to when used on an external attached drive. It is not dependent on a Trusted Platform Module (TPM) being enabled on PC's that support BitLocker natively. BitLocker is available on the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and later, and Windows Server 2008 and later. Older Windows OS's and Macintosh users can download a "BitLocker To Go Reader" utility to use with those systems.

Reader Links
Older Windows OS: http://www.microsoft.com/en-us/download/details.aspx?id=24303
Macintosh OS: http://www.m3datarecovery.com/mac-bitlocker/bitlocker-to-go-reader-for-mac-osx.html

With the increase in the use of small, large capacity USB drives, the potential for sensitive data to be lost or stolen has become a serious threat. How can you protect MIT data from loss or theft? The answer: BitLocker To Go.

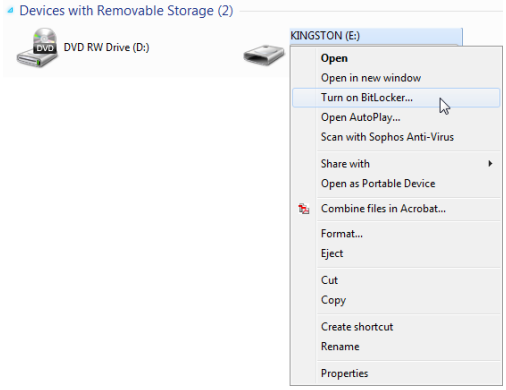
Improved for Windows 7 Ultimate and Enterprise and Windows 8.1 Pro and Enterprise. You can use BitLocker To Go to protect all file stored on a removable data drive, such as an external hard drive or USB flash drive.

To enable BitLocker encryption on a USB flash drive, perform the following steps:

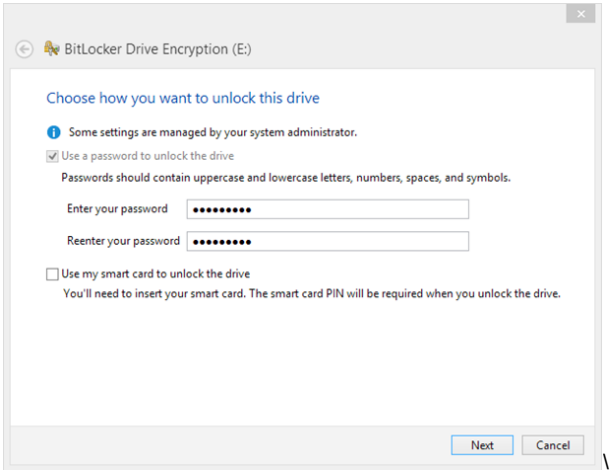
1. Insert and browse to the USB flash drive.

   Best Practice:
   As a precaution, backup all data on the drive prior to encrypting.

2. Right--click the USB flash drive or external hard drive, and then click on**Turn on Bitlocker…**



3. On the **Choose how you want to unlock this drive** window, choose **Use a password to unlock the drive**



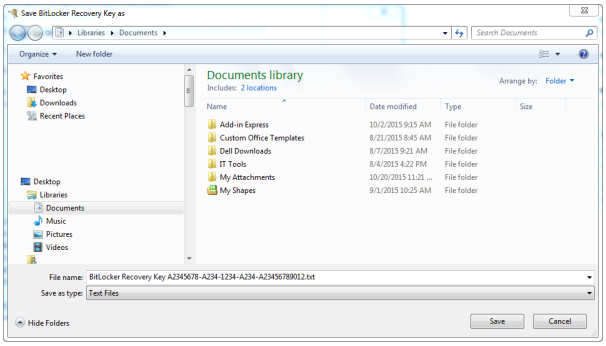
\

a. This option prompts the user for a password to unlock the drive. Passwords allow a drive to be unlocked in any location and to be shared with other people.
b. BitLocker To Go requires that passwords have at least eight characters. IS&T recommends that they contain a mixture of characters, numbers, and special characters.

4. On the **How Do You Want To Store Your Recovery Key** windows, click **Save The Recovery Key To A File.**

5. In the *Save BitLocker Recovery Key As* dialog box, choose a save location, such as your *Documents* folder, and then click **Save.**

> **Caution**
> Bitlocker suggests a name that is structured in the following way. The text, "BitLocker Recovery Key", then the Full Recovery Key ID. The first 8 alpha/numeric characters are what you will be shown when using the key recovery process. The file can be named anything, and saved anywhere you want, but you should be consistent. You may want to at the very least, incorporate those first 8 alpha/numeric characters into the name to help easily identify the key you need to use in recovery.



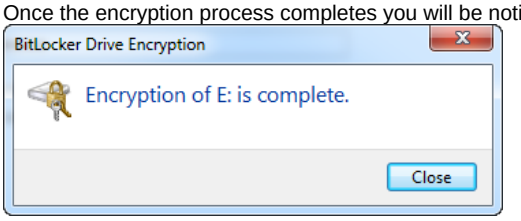
> **Note:**
> *You can also print the recovery key if you desire (from here, or by opening your saved recovery key and printing). With this recovery key file you can regain access to your encrypted USB flash drive in the event you forget your password!*

6. The message *Your Recovery Key has been saved* will appear in the dialog box and you can now click **Next** to continue.
7. On the **Are You Ready To Encrypt This Drive** window, click **Start Encrypting.**

Do not remove the USB flash drive until the encryption process is complete. How long the encryption takes depends on the size of the drive. USB drive encryption take approximately 6 to 10 minutes per gigabyte to complete. The encryption process performs the following:

   a. Creates a virtual volume with the full contents for the drive in the remaining drive space.
   b. Encrypts the virtual volume with Advanced Encryption Standard(AES) 128--?bit.

8. Once the encryption process completes you will be notified by a window.



9. Start using your encrypted drive.

Access an encrypted external storage drive

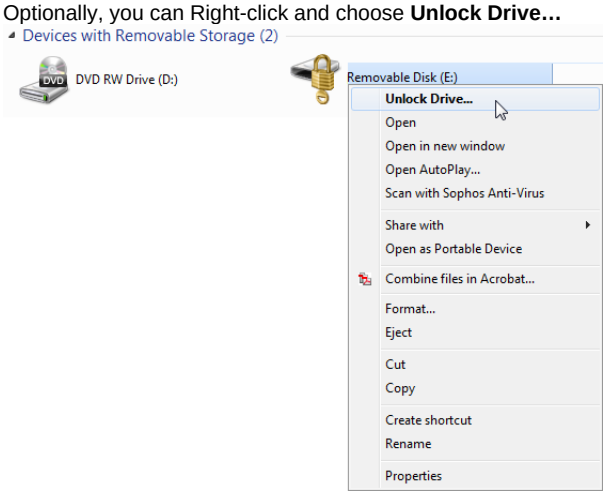
> **Important:**
> BitLocker To Go is NOT an additional application you need to install. It is how BitLocker is referred to when used on an external attached drive. It is not dependent on a Trusted Platform Module (TPM) being enabled on PC's that support BitLocker natively. BitLocker is available on the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and later, and Windows Server 2008 and later. Older Windows OS's and Macintosh users can download a "BitLocker To Go Reader" utility to use with those systems.
>
> Reader Links
> Older Windows OS: http://www.microsoft.com/en-us/download/details.aspx?id=24303
> Macintosh OS: http://www.m3datarecovery.com/mac-bitlocker/bitlocker-to-go-reader-for-mac-osx.html

Once you have encrypted your external drive and saved a recovery key, you're ready to go. Your drive will be unlocked for as long as it is connected to your computer, but at some point, you may reboot, or need to eject it. After this happens, you will be required to enter your password again.

Scenario 1 – Reboot

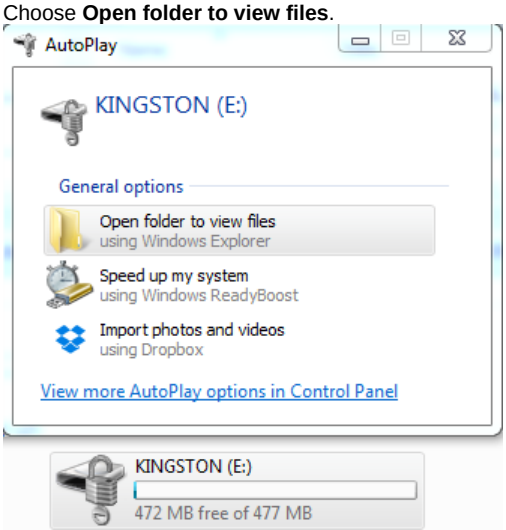
1. Browse to your Computer, and you will find your external USB drive is locked. It will NOT automatically prompt you for a password.
   a. Double-click on the locked drive icon.

b. Optionally, you can Right-click and choose **Unlock Drive…**



2. Enter your password, and click **Unlock**.

3. Choose **Open folder to view files**.



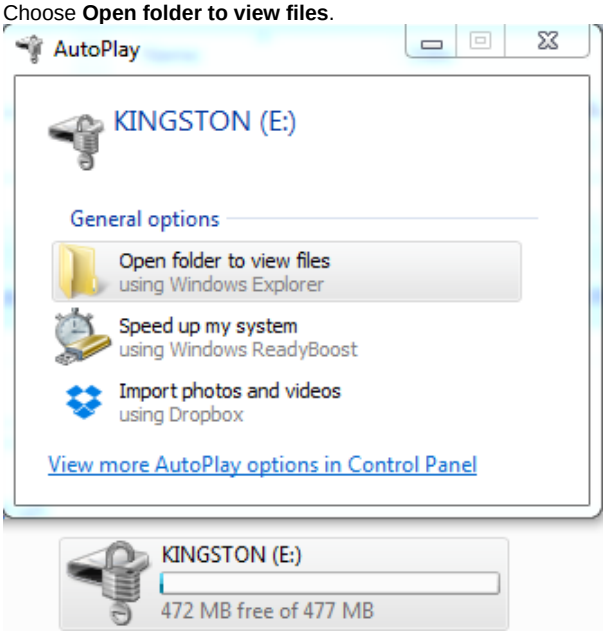
4. Start using your drive.

Scenario 2 – You inserted your external drive in the same/other machine

5. The *BitLocker Drive Encryption* dialog box will automatically pop-up.

6. Enter your password, and click **Unlock**.

7. Choose **Open folder to view files**.



8. Start using your drive.

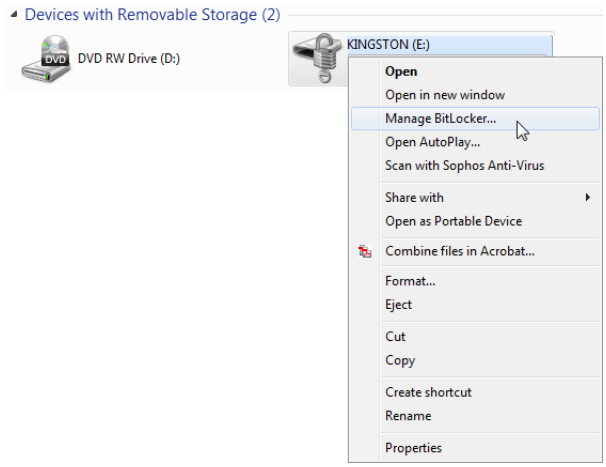
Manage an encrypted external drive

Important:
BitLocker To Go is NOT an additional application you need to install. It is how BitLocker is referred to when used on an external attached drive.It is not dependent on a Trusted Platform Module (TPM) being enabled on PC's that support BitLocker natively. BitLocker is available on the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and later, and Windows Server 2008 and later. Older Windows OS's and Macintosh users can download a "BitLocker To Go Reader" utility to use with those systems.

Reader Links
Older Windows OS: http://www.microsoft.com/en-us/download/details.aspx?id=24303
Macintosh OS:http://www.m3datarecovery.com/mac-bitlocker/bitlocker-to-go-reader-for-mac-osx.html

When you have an external encrypted drive in your computer and unlocked, there are some options for managing BitLocker for this drive. Below are some examples of things you can manage.
Common method for All Scenario's below -- Access the *Manage BitLocker…* dialog box.

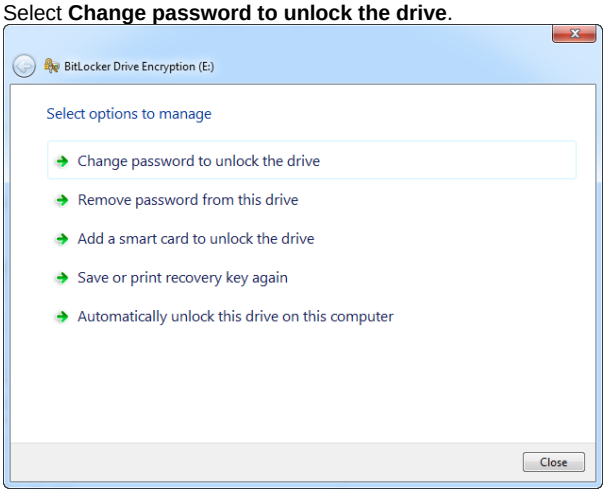
1. Right click on your unlocked encrypted drive and select **Manage BitLocker…**



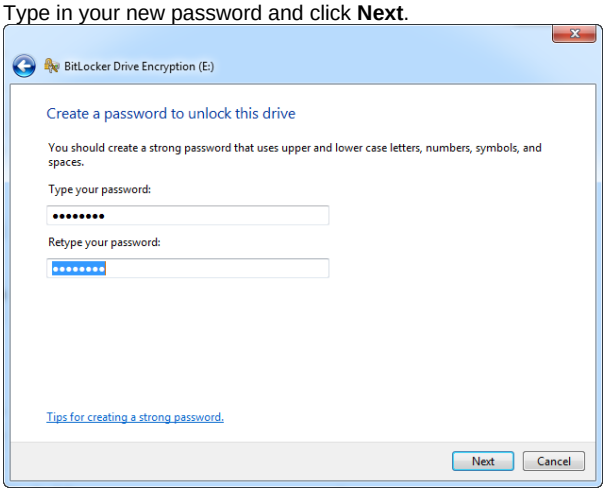
2. Select options to manage
    a. Change password to unlock the drive
    b. Remove password from this drive
    c. Add a smart card to unlock the drive
    d. Save or print recovery key again
    e. Automatically unlock this drive on this computer

Scenario A – Change password to unlock the drive

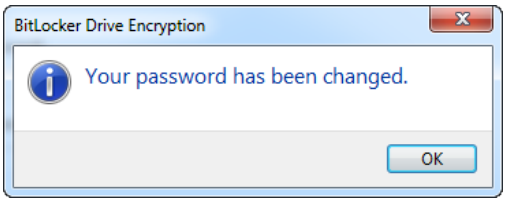
1. Select **Change password to unlock the drive**.



2. Type in your new password and click **Next**.



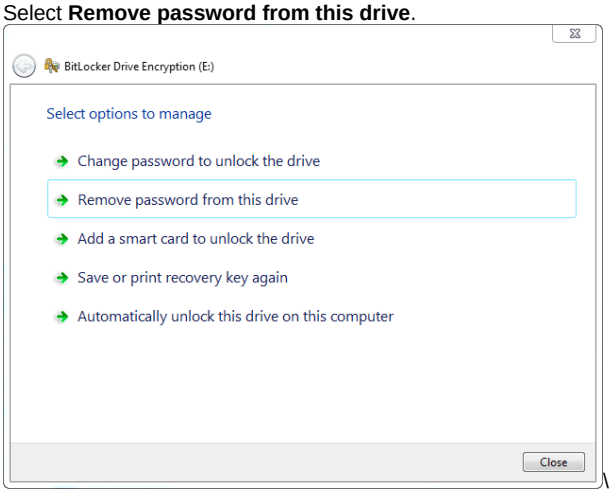
3. You will receive the following confirmation. Click **OK**.



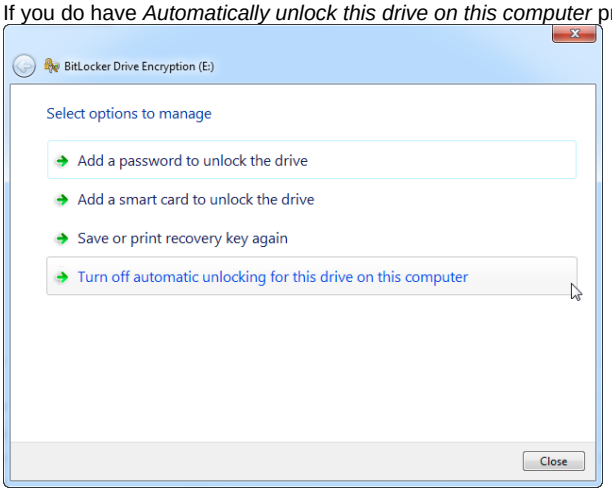
4. You will be returned to the *Select options to manage* dialog box. Click **Close** if you have no other options to manage.

Scenario B – Remove password from this drive

1. Select **Remove password from this drive**.

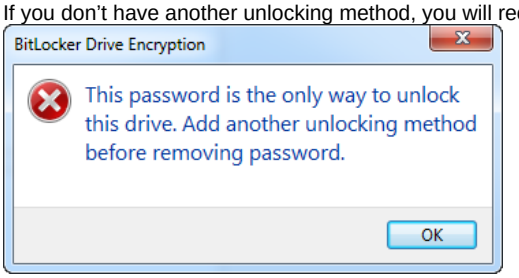


   a. If you do have *Automatically unlock this drive on this computer* previously set, you will receive the following message.



> **Note:**
> The *Change password to unlock the drive* option goes away, and you can click **Close** now.

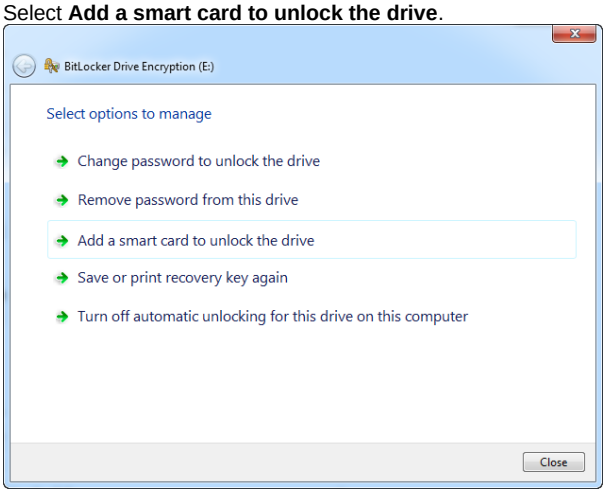
   b. If you don't have another unlocking method, you will receive the following message. Click **OK**.



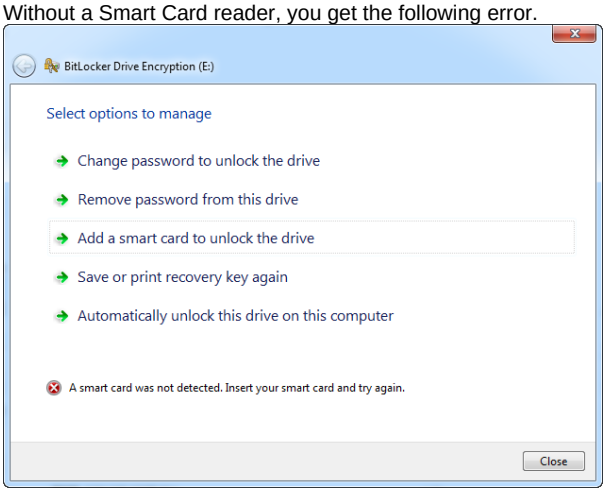
2. You will be returned to the *Select options to manage* dialog box.
3. You will now have to set **Automatically unlock this drive on this computer**, for this to work. (See Scenario E below to see how to do this)
4. Return to Step 1 to remove the password now.

Scenario C – Add a smart card to unlock the drive (NOT Supported)

1. Select **Add a smart card to unlock the drive**.



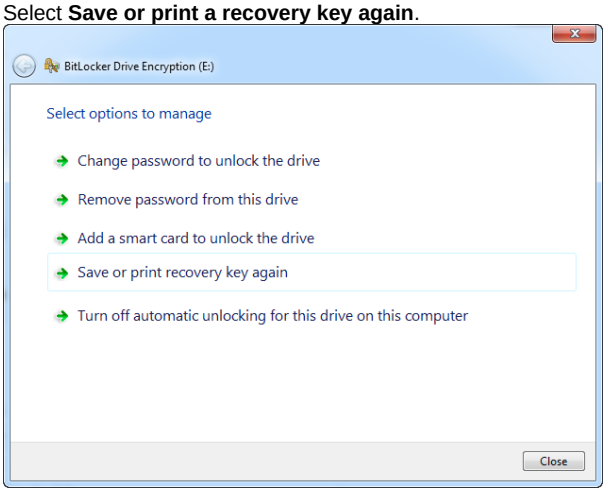
2. Without a Smart Card reader, you get the following error.



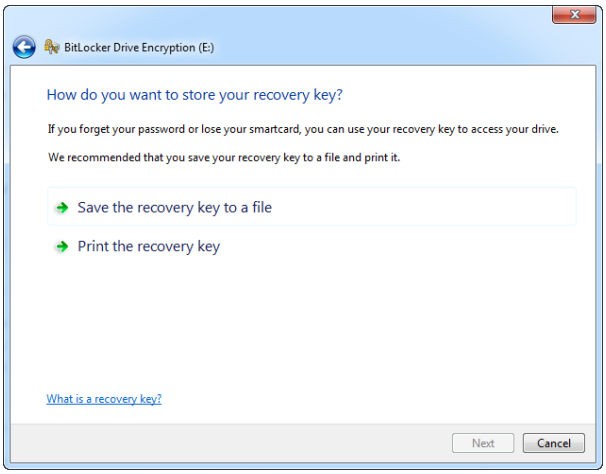
3. You will still be in the *Select options to manage* dialog box, so you can click **Close** if you have no other options to manage.

Scenario D – Save or print recovery key again

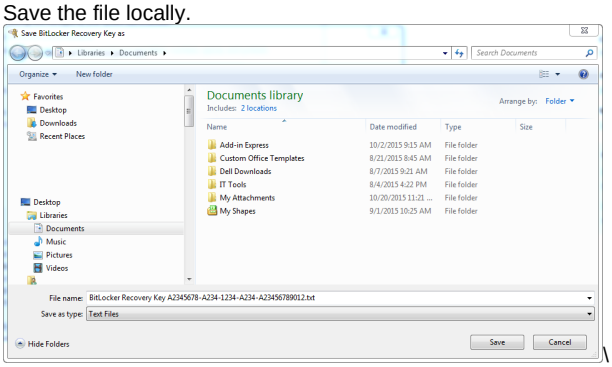
1. Select **Save or print a recovery key again**.



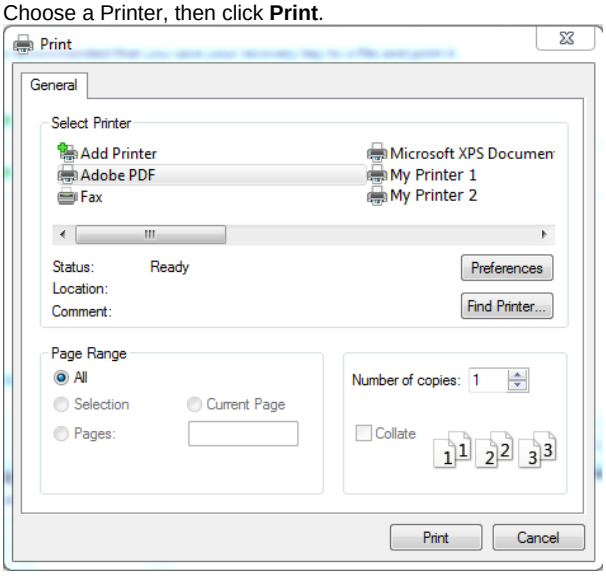
2. Select **Save the recovery key to a file**.



3. Save the file locally.



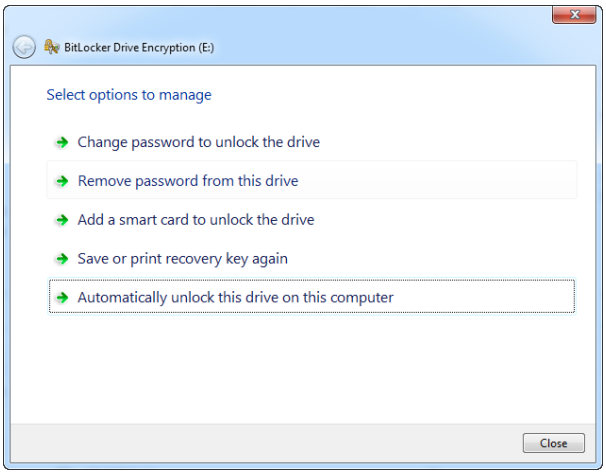
   a. In the *Save BitLocker Recovery Key As* dialog box, choose a save location, such as your *Documents* folder, and then click **Save**. BitLocker suggests a name but you can name this anything you will remember. It would be nice to at least leave the first alphanumeric series of 8 numbers as this will be useful in the recovery process.
   b. You will be returned to the *Select options to manage* dialog box. Click **Close** if you have no other options to manage.
4. Select **Print the recovery key**.
5. Choose a Printer, then click **Print**.



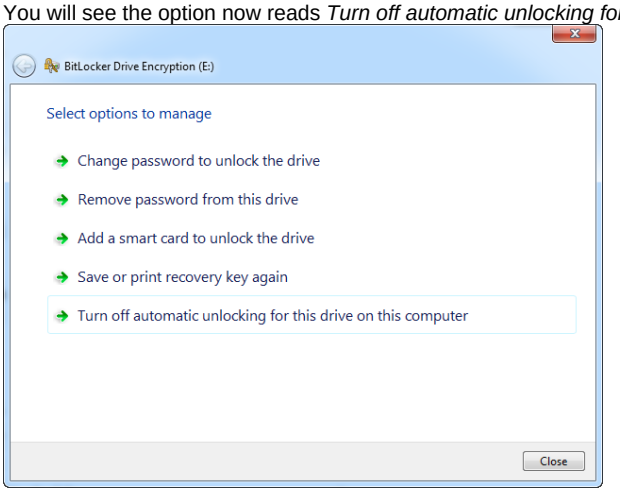
6. Click **Close** if you have no other options to manage.

Scenario E – Automatically unlock this drive on this computer

1. Select **Automatically unlock the drive on this computer**.



2. You will see the option now reads *Turn off automatic unlocking for this drive on this computer*.



3. You can click **Close** if you have no other options to manage.

Recover from key to an encrypted external storage drive

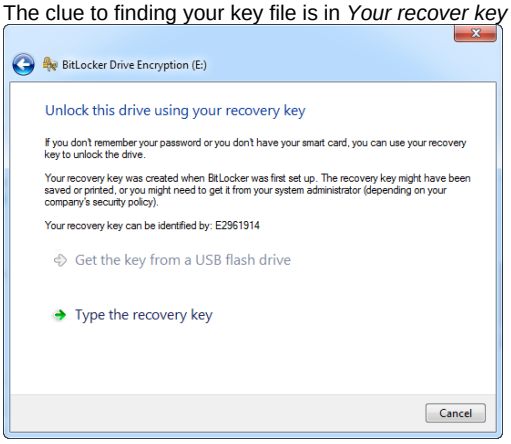
Important:
BitLocker To Go is NOT an additional application you need to install. It is how BitLocker is referred to when used on an external attached drive. It is not dependent on a Trusted Platform Module (TPM) being enabled on PC's that support BitLocker natively. BitLocker is available on the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and later, and Windows Server 2008 and later. Older Windows OS's and Macintosh users can download a "BitLocker To Go Reader" utility to use with those systems.

Reader Links
Older Windows OS: http://www.microsoft.com/en-us/download/details.aspx?id=24303
Macintosh OS: http://www.m3datarecovery.com/mac-bitlocker/bitlocker-to-go-reader-for-mac-osx.html

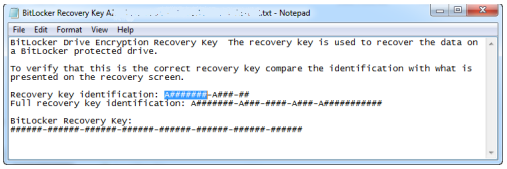
When you forget your password, and need to gain access to your encrypted drive, you can gain access with your recovery key.

1. Insert the external drive, and click on **I forgot my password**.

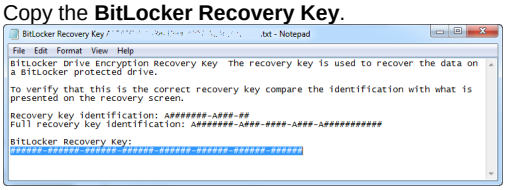
2. The clue to finding your key file is in *Your recover key can be identified by:*. Make note of this.



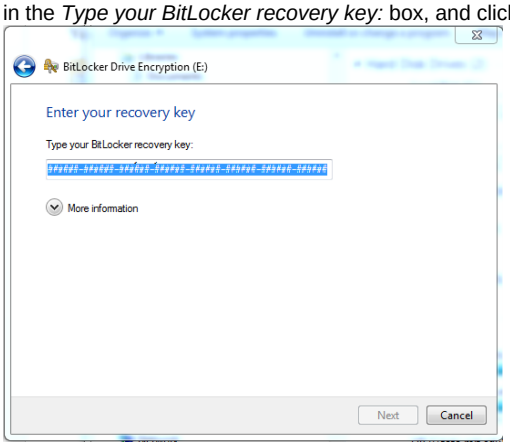
3. Find and open the recovery key file on your computer.
    a. Confirm that the id matches.



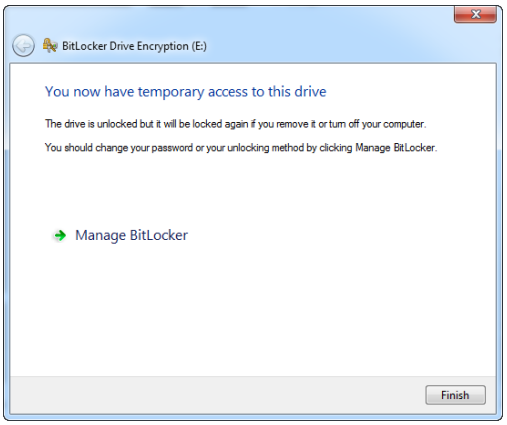
    b. Copy the **BitLocker Recovery Key**.



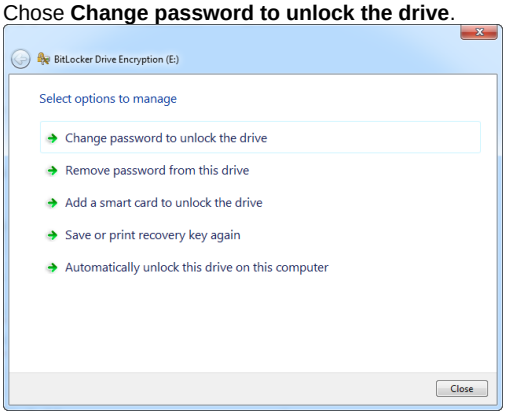
4. Return to the *Unlock this drive using your recovery key* dialog box (see step 2), click on **Type the recovery key**. Pasted the recovery key in the *Type your BitLocker recovery key:* box, and click **Next**.



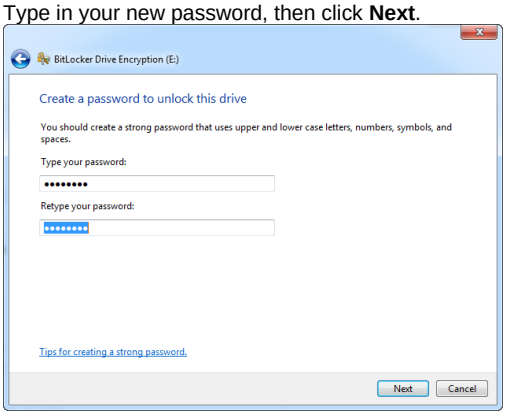
5. You are now have Temporary access to the drive and must reset the password. Click on **Manage BitLocker**.



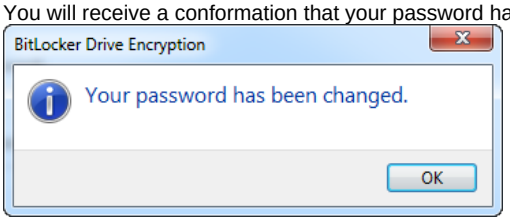
6. Chose **Change password to unlock the drive**.



7. Type in your new password, then click **Next**.



8. You will receive a conformation that your password had been changed. Click **OK** to close this dialog box.



9. You will be returned to the dialog box in step 6. Click on **Close** now.
10. You will be returned to the dialog box in step 5. Click on **Finish** now.
11. You will now be presented with your open drive in a new explorer window. You can now work with the contents.

Decrypt an external storage drive

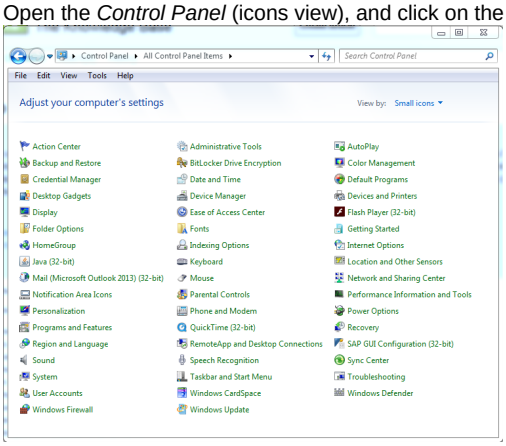
Important:
BitLocker To Go is NOT an additional application you need to install. It is how BitLocker is referred to when used on an external attached drive. It is not dependent on a Trusted Platform Module (TPM) being enabled on PC's that support BitLocker natively. BitLocker is available on the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and later, and Windows Server 2008 and later. Older Windows OS's and Macintosh users can download a "BitLocker To Go Reader" utility to use with those systems.

Reader Links
Older Windows OS: http://www.microsoft.com/en-us/download/details.aspx?id=24303
Macintosh OS: http://www.m3datarecovery.com/mac-bitlocker/bitlocker-to-go-reader-for-mac-osx.html

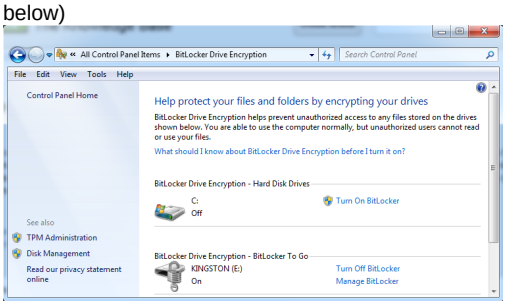
At some time, you may want to turn off the encryption on your external encrypted drive. Here's the step on how to do that.

Turn Off BitLocker to Decrypt Removable Drive

1. Connect the removable hard drive or USB flash drive.
2. Type in your password, and click on the **Unlock** button.
3. Open the *Control Panel* (icons view), and click on the **BitLocker Drive Encryption** icon.



4. Click on **Turn Off BitLocker** for the drive letter for the removable hard drive or USB flash drive that you want to decrypt. (See screenshot below)

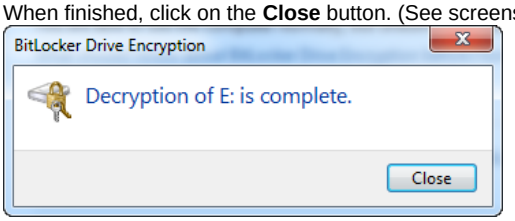


5. Click on the **Decrypt Drive** button. (See screenshot below)

Note:
This may take a while to finish.

6. BitLocker will now start decrypting the drive. (See screenshot below)

7. When finished, click on the **Close** button. (See screenshot below)



8. The **Control Panel** and **Computer** will now have the Turn On BitLocker option again.
9. You're done. The drive is now decrypted with BitLocker To Go turned off, and your data intact.