Encrypting with BitLocker To Go for removable devices under Windows 7
(BitLocker To Go User Guide)

1. Introduction
   BitLocker To Go—a new feature of Windows 7—is a full-disk encryption protection technology for removable storage devices that are connected to one of the USB ports on your computer (referred as either USB drive or drive hereafter).

   Basically, BitLocker To Go allows you to encrypt a USB drive and restrict access with a password. When you connect the encrypted USB drive to a Windows 7 computer, you will be prompted for the password and upon successfully entering it, you can read and write to the drive as usual.

   During the encryption process, Windows 7 installs a special reader on the USB drive. When you connect the encrypted USB drive to a computer running Windows Vista, the BitLocker To Go Reader takes control, prompts for the password, and then basically makes the USB drive a read-only device.

2. Turning on BitLocker To Go for a USB Drive
   i. Insert a USB Drive to a computer running Windows 7 Enterprise or Windows 7 Ultimate, right-click on the drive icon and select the “Turn on BitLocker” command from the menu.
ii. Once the initialization process is completed, BitLocker To Go will prompt you to set up a password that is used to unlock the drive.

![BitLocker Drive Encryption (F:)]

Choose how you want to unlock this drive

- Use a password to unlock the drive
  - Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.
  - Type your password: 
  - Retype your password: 

- Use my smart card to unlock the drive
  - You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?

![BitLocker Drive Encryption (F:)]

iii. After setting up a password, BitLocker To Go will prompt you to store or print the recovery key that is used to unlock the drive in case you forget the password one day.

![BitLocker Drive Encryption (F:)]

How do you want to store your recovery key?

If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

We recommend that you save your recovery key to a file and print it.

- Save the recovery key to a file
- Print the recovery key

What is a recovery key?
iv. You will be prompted to start the encryption process.

v. During the encryption process, a progress monitor will be shown. The amount of time that it will take to complete the process varies, depending mainly on the size of your drive.
vi. Once the encryption is complete, BitLocker To Go displays a confirmation dialog box and a lock icon will be shown on the Drive.

![BitLocker Drive Encryption]

Encryption of F: is complete.

vii. If you use Windows Explorer to explore the encrypted drive, you will find the BitLocker To Go Reader and a Read Me shortcut linking to Microsoft’s BitLocker website.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>BitLockerToGo</td>
<td>7/14/2009 9:26 AM</td>
<td>Application</td>
<td>251 KB</td>
<td></td>
</tr>
<tr>
<td>Read Me</td>
<td>6/11/2009 5:43 AM</td>
<td>Internet Shortcut</td>
<td>1 KB</td>
<td></td>
</tr>
</tbody>
</table>

The BitLocker To Go Reader is a program for you to unlock encrypted drives and copy its content to computers running Windows Vista (although Windows 7 does not need it.) Therefore, you should not remove this program. If you accidentally delete it, you may download it from the Microsoft website or copy it from another BitLocker To Go encrypted drive.

3. **Using a BitLocker To Go encrypted drive in Windows 7**

When a BitLocker To Go encrypted drive is plugged in any Windows 7 system (no need to be Enterprise or Home Ultimate), a dialog window will appear, informing you that the drive is protected by BitLocker Drive Encryption and waiting for you to enter the password.
After typing the password and clicking the Unlock button, you will be able to access the drive and its content as usual.
4. **Using a BitLocker To Go encrypted drive in Windows Vista**

A BitLocker To Go encrypted drive will become Read-Only in the Windows Vista environments. When you insert the encrypted drive in a computer running Windows Vista, you will be informed that the drive is protected by BitLocker Drive Encryption as shown in 3 above. After entering the correct password to unlock the drive, you will be able to copy the files stored there. However, you will not be able to modify the files or save other files to the encrypted drive. You should remember that duplicated files created in the new location will not be protected by BitLocker even though the original files will still be protected on the encrypted drive.

The BitLocker To Go Reader is not supported on removable drives formatted with NTFS.

5. **Recovering the encrypted USB drive using BitLocker recovery key**

If you forget the password of the encrypted drive, the BitLocker recovery key saved or printed in 2 (iii) above will help you unlock the drive and create a new password for the drive.

i. Plug the encrypted USB drive in Windows 7 and click “I forget my password”
ii. Click “Type the recovery key”

iii. Enter the BitLocker recovery key and click “Next”

If you have saved the recovery key in a file, you can simply copy and paste it; otherwise, you have to enter the long key carefully.
iv. Click “Manage BitLocker”

![Manage BitLocker dialog box](image1)

You now have temporary access to this drive

The drive is unlocked but it will be locked again if you remove it or turn off your computer.

You should change your password or your unlocking method by clicking Manage BitLocker.

![Manage BitLocker link](image2)

v. Click “Change password to unlock the drive”

![Change password dialog box](image3)

Select options to manage

- Change password to unlock the drive
- Remove password from this drive
- Add a smart card to unlock the drive
- Save or print recovery key again
- Automatically unlock this drive on this computer

![Change password options](image4)
vi. Type the new password and click “Next”

6. **Forgetting both the password and the recovery key**

   If you have lost both the password and the recovery key, you will lose your data forever as you cannot unlock the drive. Therefore, you are recommended to memorize the password and keep the printed or saved recovery key in a safe place.

   If you have really lost your password and recovery key and want to refresh the USB drive for use, you may follow the procedure below to format it.
i. Right-click on the USB drive icon and select “Format” command on the menu
ii. Click “Start”

![Format Removable Disk dialog box]

iii. Click “OK” to format the USB drive

![Format Removable Disk dialog box with warning]

WARNING: Formatting will erase ALL data on this disk. To format the disk, click OK. To quit, click CANCEL.
iv. Click “OK”

v. Click “Close” and the USB drive has been refreshed