

# **E-Pollbook Flash Drive Guide for BitLocker**



**Michigan Department of State  
Bureau of Elections**

**May 2016**

## **E-Pollbook Flash Drive Guide for BitLocker - Table of Contents**

Introduction .....	3
BitLocker .....	3
Putting BitLocker To Go on a flash drive .....	4
Unlocking a BitLocker Flash Drive.....	7
Changing the BitLocker Password .....	8
Forgot the Password .....	8
Change the Existing Password.....	9

# E-Pollbook Flash Drive Guide for BitLocker

---

## Introduction

The encrypted flash drive is used to securely store data and transfer files back and forth between the QVF or EMP computer and the EPB laptop. The encrypted flash drive is the key to maintaining security with the E-Pollbook. Passwords should **never** be kept with flash drives.

There are two kinds of encryption software supported by the Bureau of Elections (BOE) and the QVF Help Desk. They are BitLocker and V-Safe 100. The steps for logging into these 2 kinds of encryption software are different.

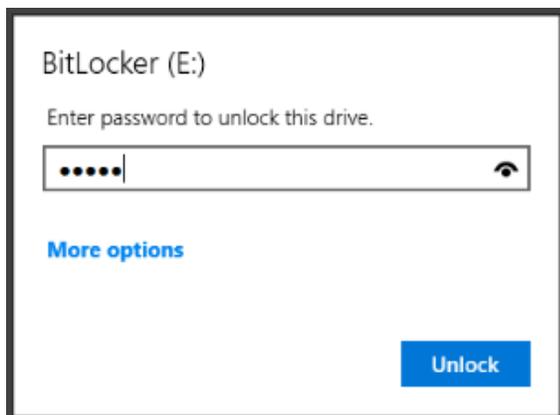
This guide contains instructions for using a flash drive with BitLocker on a Windows 10 computer.

Instructions for using a BitLocker flash drive on a Windows 10 E-Pollbook can be found in the [Electronic Pollbook User Manual for Windows 10 & BitLocker](#).

Instructions for using a Verbatim flash drive with V-Safe 100 software on a Windows 7 computer can be found in the [Electronic Pollbook User Manual for Windows 7 and V-Safe 100](#).

## BitLocker

BitLocker is encryption software from Microsoft for encrypting data on computers and external storage devices such as flash drives.



In order to save or open files from a drive encrypted with BitLocker, you must first unlock the drive by entering the encryption password. Without the password or the Recovery Key, the drive is inaccessible. This ensures that the voter data saved to these flash drives is always protected in case it is lost or stolen.

## Putting BitLocker To Go on a flash drive

BitLocker To Go (BitLocker) is encryption software used to encrypt a flash drive to keep the data on it stored securely.

In order to put BitLocker on a flash drive you must have a computer with one of the following operating systems:

- Windows Vista Ultimate
- Windows 7 Ultimate
- Windows 7 Enterprise
- Windows 8 Professional
- Windows 8 Enterprise
- Windows 8.1 Professional
- Windows 8.1 Enterprise
- **Windows 10 Professional** – Includes EPB laptops (most Compaq 515s, HP 635s and HP ProBook 4535s) that upgraded from Windows 7 to Windows 10
- Windows 10 Enterprise

Once encrypted, a BitLocker flash drive can be used on any Windows 7, 8 or 10 computer.

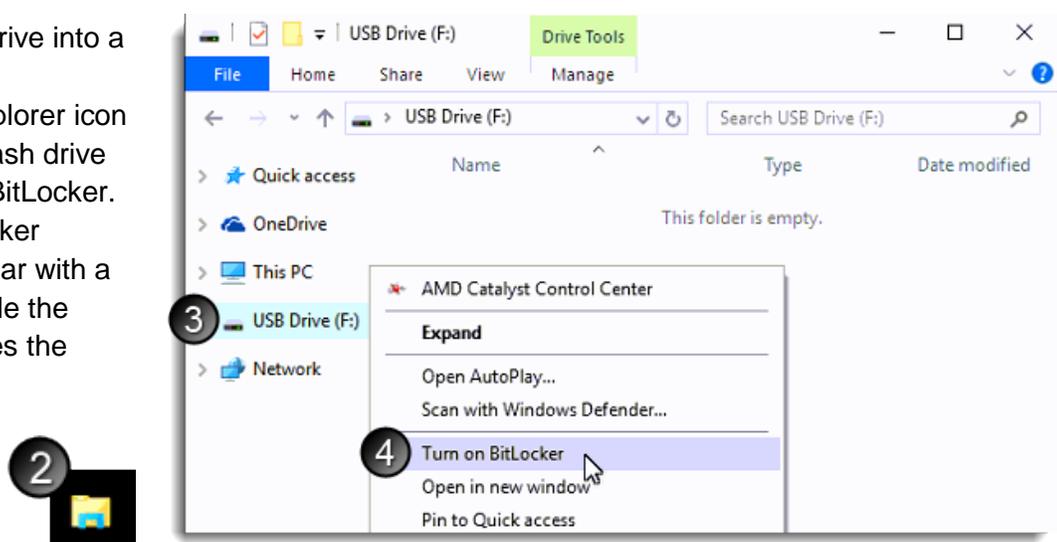
### To determine the operating system on a computer:

1. Type “operating system” in the search field. If you don’t see a search field in the lower-left corner of the screen, click the Home or Start button in the lower-left of the screen to bring up the search field.
2. Click on the match of either “About your PC” or “Show which operating system...”
3. Find the operating system listed under the Edition heading

### To encrypt a flash drive with BitLocker:

**Note:** These instructions are for Windows 10 Professional or Enterprise

1. Insert the flash drive into a USB port
2. Click the File Explorer icon
3. Right-click the flash drive
4. Select Turn On BitLocker.  
A Starting BitLocker window will appear with a progress bar while the software initializes the drive.



5. When available, select the top option, “Use a password to unlock the drive”
6. Enter a strong password, and re-enter the password to confirm it
7. Click Next

You will then be prompted to save or print the recovery key. When you forget the password, the Recovery Key is used to access the flash drive so you can change the password.

BitLocker Drive Encryption (D:)

Choose how you want to unlock this drive

**5**  Use a password to unlock the drive  
Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password  **6**

Reenter your password

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

**7** Next Cancel

8. Choose “Save to a file” and then browse to the location you want to save the file
  - The default location is in My Documents
  - You can change the file name; however, you should be descriptive in the name, example: BitLockerEPBPCT1
9. Click Save
10. Click Next

BitLocker Drive Encryption (D:)

How do you want to back up your recovery key?

**9** **1** Your recovery key has been saved ✓  
If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your Microsoft account

→ Save to a file **8**

→ Print the recovery key

[What is a recovery key?](#)

**10** Next Cancel

11. Make sure the first option is selected, “Encrypt used disk space only”, and click Next

BitLocker Drive Encryption (D:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info.

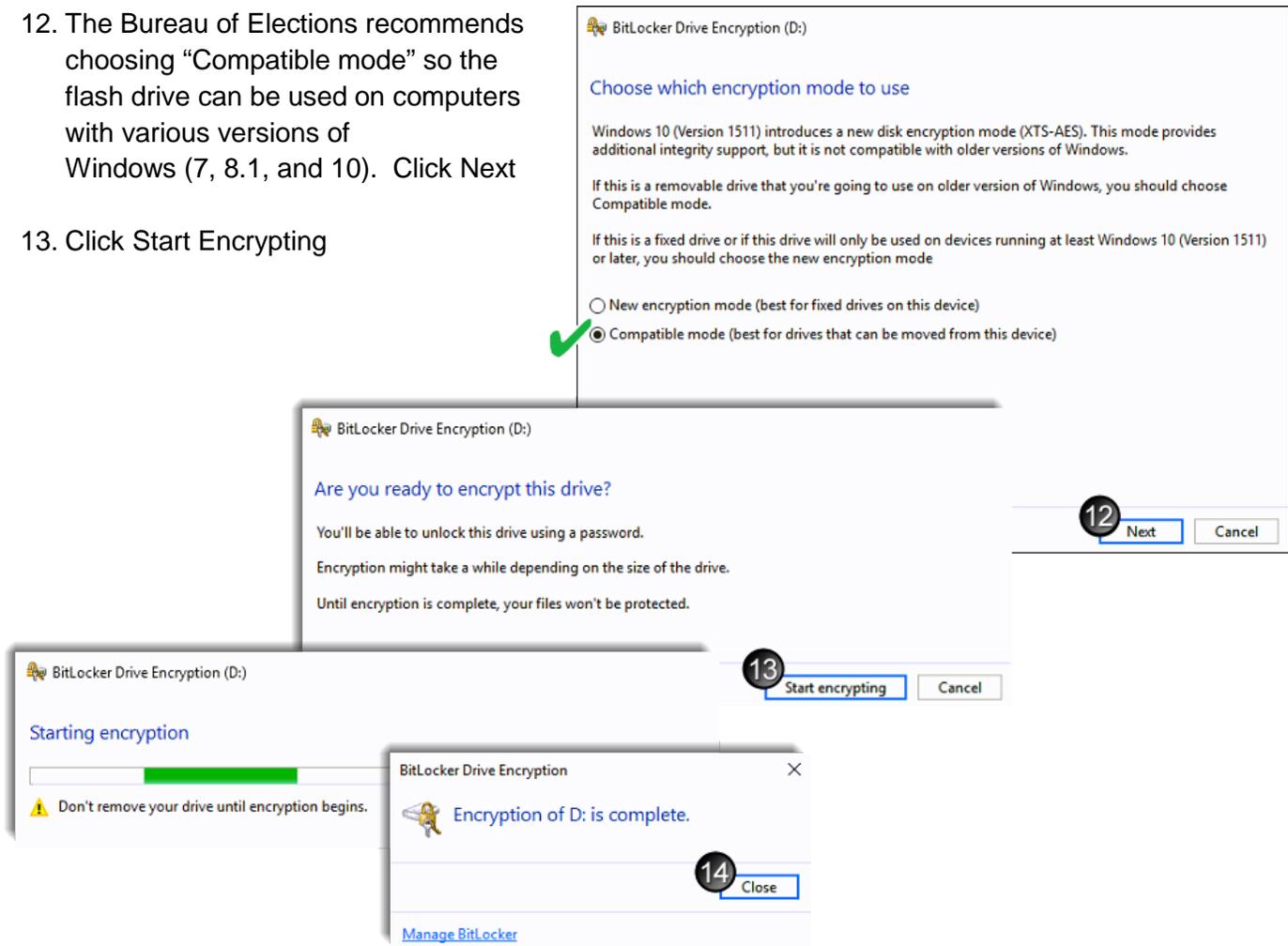
**11**  Encrypt used disk space only (faster and best for new PCs and drives)

Encrypt entire drive (slower but best for PCs and drives already in use)

**11** Next Cancel

12. The Bureau of Elections recommends choosing “Compatible mode” so the flash drive can be used on computers with various versions of Windows (7, 8.1, and 10). Click Next

13. Click Start Encrypting



BitLocker software begins encrypting the drive. **DO NOT REMOVE THE DRIVE UNTIL THE ENCRYPTION PROCESS IS COMPLETE.** If you must remove the flash drive before the process is complete, you must click Pause before removing the device. Larger capacity flash drives will take longer to encrypt. The process should take between 10-25 minutes to complete.

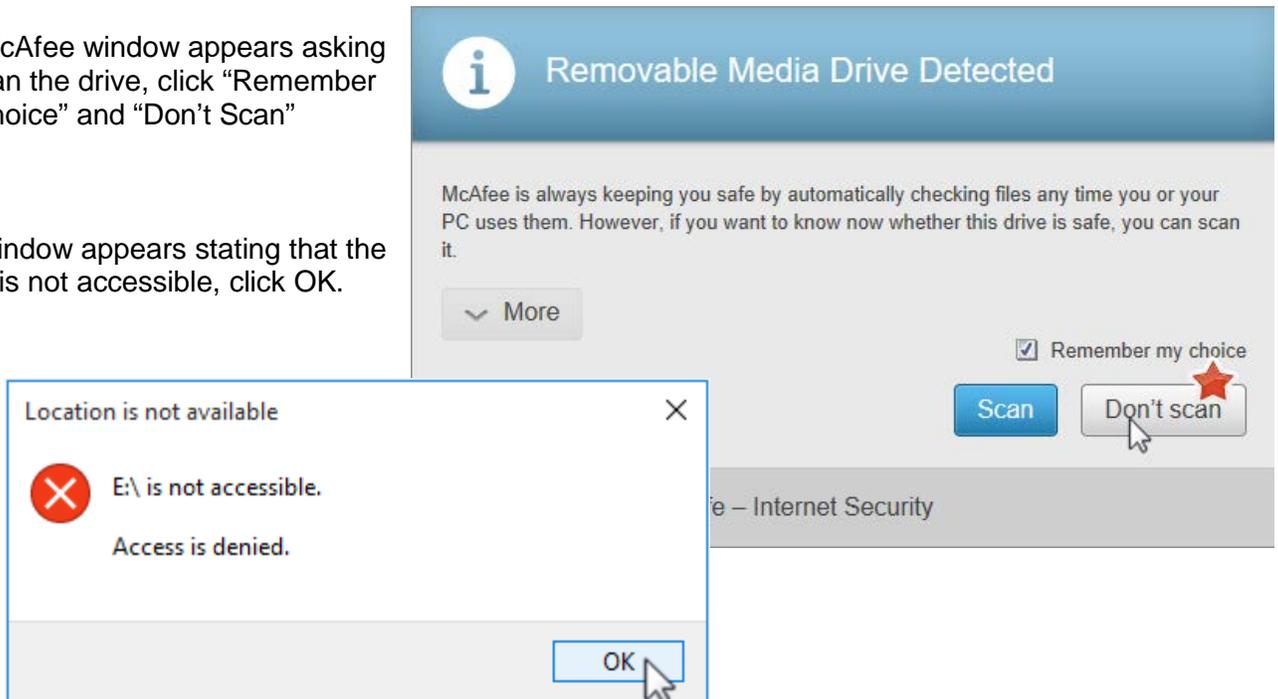
14. When the confirmation window says that encryption of the drive is complete, click Close to finish.

## Unlocking a BitLocker Flash Drive

Once the flash drive is inserted into a USB port on the laptop, the BitLocker password must be entered in order to access the encrypted flash drive.

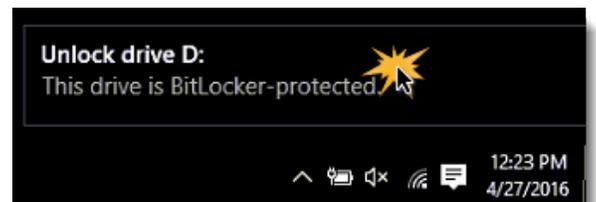
If a McAfee window appears asking to scan the drive, click “Remember my choice” and “Don’t Scan”

If a window appears stating that the drive is not accessible, click OK.

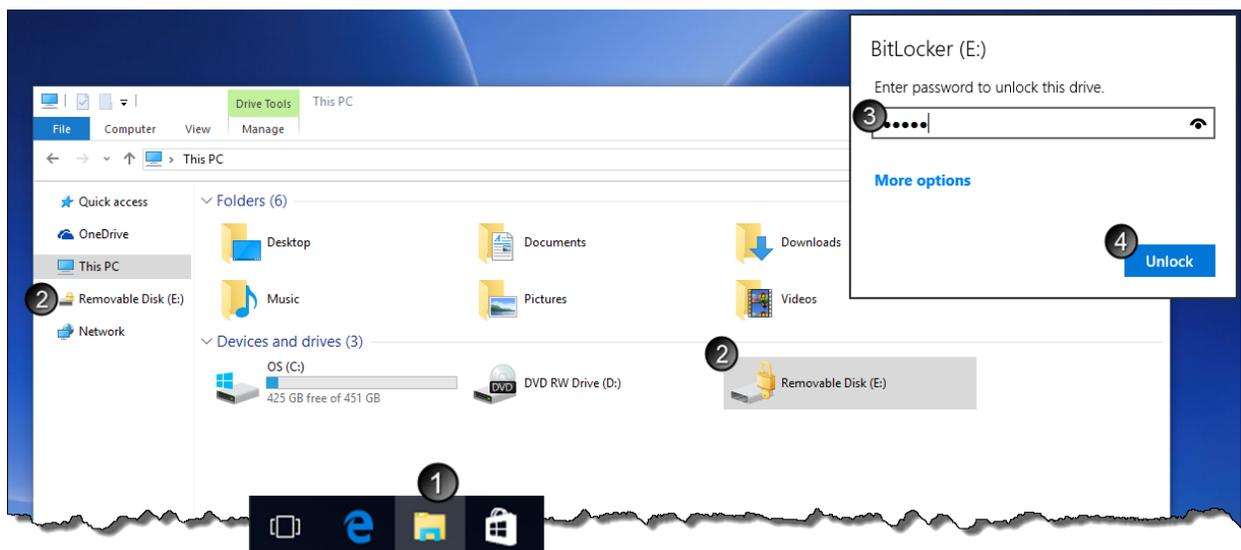


Then proceed with the following steps to unlock the drive.

If an “Unlock Drive” pop-up appears in the lower right corner of the screen, click the message, then skip to Step 3 below, otherwise:



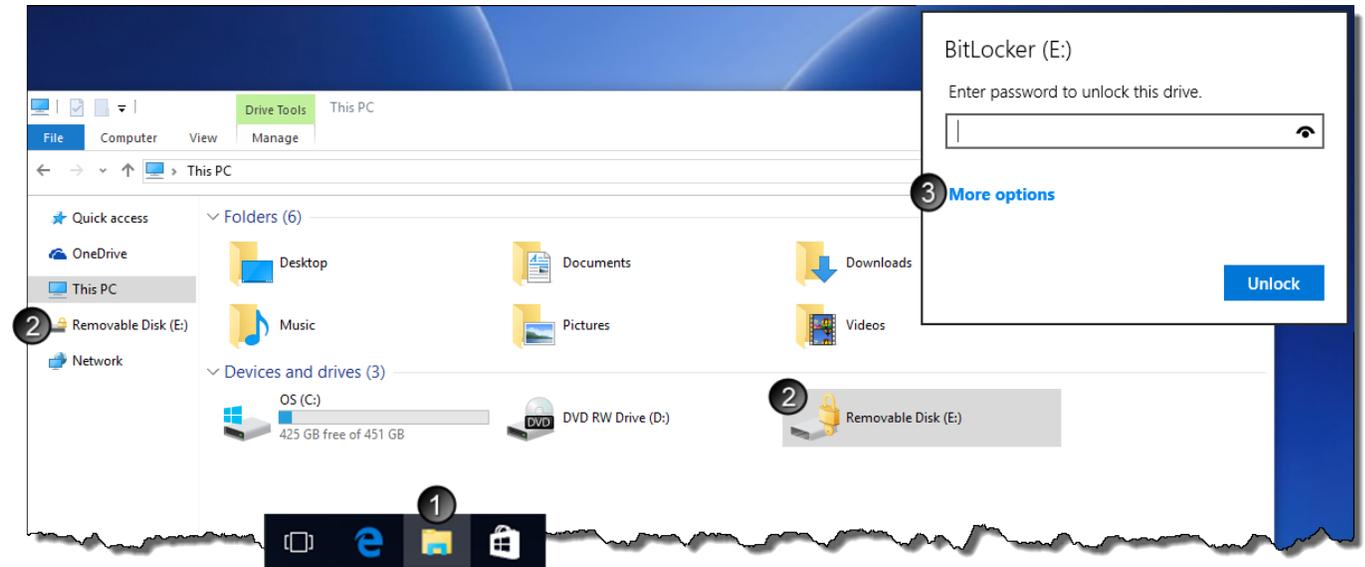
1. Open Windows file explorer
2. Click on Removable Disk or USB Drive
3. Enter the password
4. Click Unlock



## Changing the BitLocker Password

### Forgot the Password

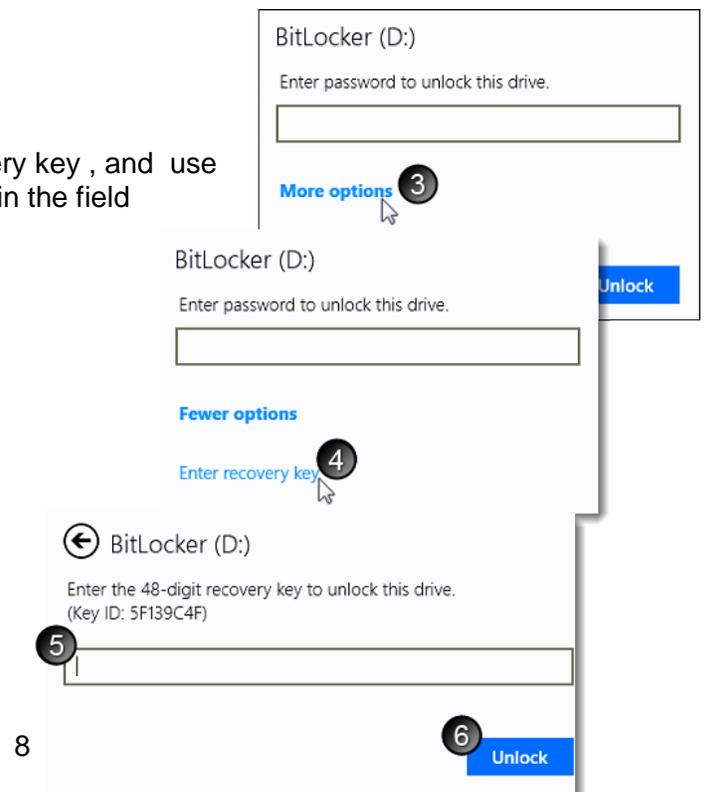
If you are unable to log into the flash drive, you must use the Recovery Key to access the flash drive, then proceed to change the password. The Recovery Key can be used to access the flash drive on any computer. However, to make a new password, these steps must be performed on a computer with an operating system listed on pg. 4 of this manual.



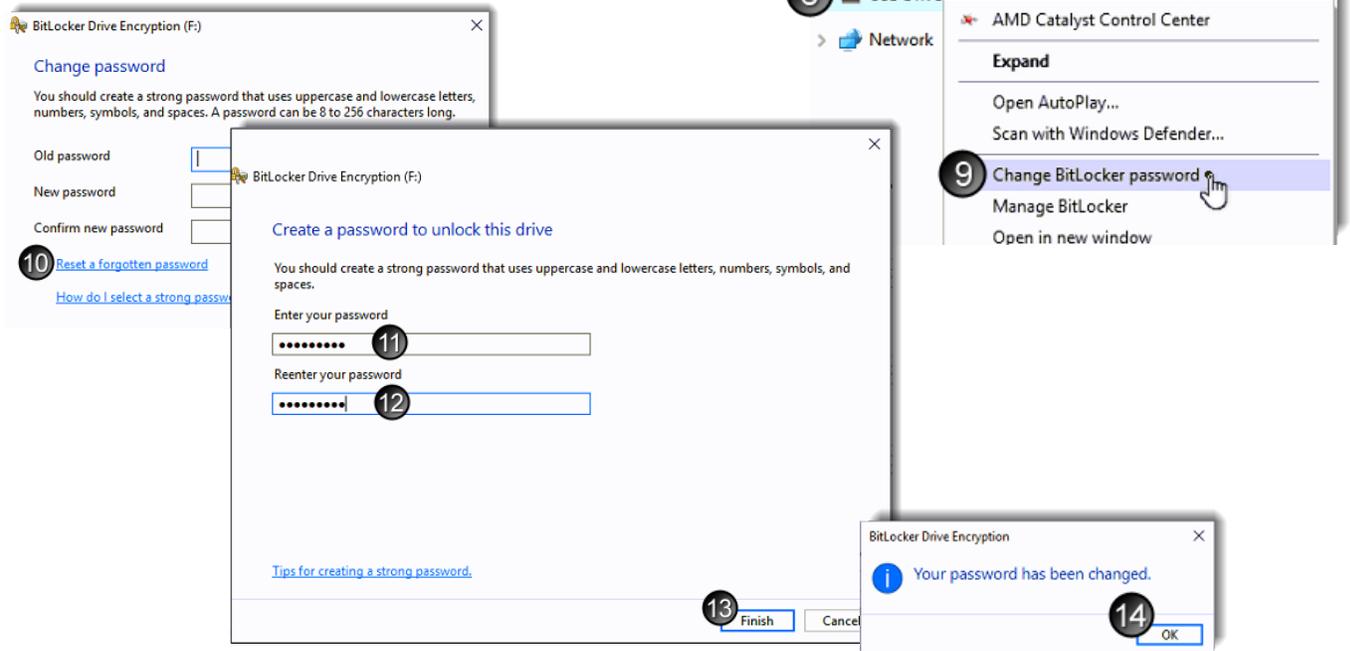
**Note:** It is helpful to locate the Recovery Key before beginning these steps

1. Open Windows File Explorer
2. Click on Removable Disk or USB Drive
3. Click More Options
4. Click Enter Recovery key
5. Type the Recovery Key, or copy the recovery key , and use Ctrl + V on your keyboard to paste the key in the field
6. Click Unlock

Proceed to the next page to reset the password.



7. Open File Explorer if the window is not open already.
8. Right-click the Removable Disk or USB Drive
9. Select Change BitLocker Password
10. Click Reset a forgotten password
11. Enter a new password
12. Reenter the new password
13. Click Finish
14. Click OK



## Change the Existing Password

**Note:** Passwords can only be changed using computers with an operating system listed on pg. 4 of this manual.

After logging into to the flash drive (see steps 1-3 pg. 8) perform steps 7-9 shown above then proceed with the following:

1. Enter the current/old password
2. Enter the new password
3. Confirm the new password
4. Click Change Password
5. Click Close

