

Enabling BitLocker on the BIOFIRE® TORCH® Base

Contents

1.	Introduction	2
2.	Scope	2
3.	What's Needed?.....	2
4.	How to Configure BitLocker on C: Drive.....	3
5.	How to Configure BitLocker on D: Drive.....	14
6.	Disabling BitLocker	26
7.	Technical Support Contact Information	37
8.	Frequently Asked Questions (FAQs).....	37
9.	Appendix	37



1. Introduction

Windows BitLocker Drive Encryption is a data protection feature that integrates with the Windows operating system. It helps protect against data theft or exposure from lost, stolen, or inappropriately decommissioned computers by encrypting the entire operating system drive, including all user and system files.

bioMérieux has provided the following instructions to configure this optional feature on the TORCH Base in this Technical Note.

Systems equipped with a Trusted Platform Module (TPM), particularly TPM 2.0, can take advantage of enhanced security features and simplified user experience when using BitLocker. TPM enables secure key storage and allows the system to automatically unlock the encrypted drive during startup.

NOTE: During the BitLocker encryption process, the TORCH System cannot perform any patient tests. This process may take several hours depending on the amount of data on the hard drive. The Base must be kept **ON** throughout this entire process.

NOTE: It is the customer's responsibility to securely store and maintain the BitLocker recovery key. It is strongly recommended that a copy of the recovery key be provided to the customer's IT department.

NOTE: BitLocker must be disabled prior to returning the system for service. Refer to Section 6 for instructions on how to disable BitLocker.

2. Scope

This document applies to the TORCH Base system.

System Identification Note:

The TORCH Base system referenced in this document is identified as either:

- **TORCH Base v2** and, or
- A system that has been designed or upgraded to use the **AIMB-278 motherboard**.

NOTE: Encrypting the D: drive is optional but recommended. If the D: drive is encrypted, the C: drive must also be encrypted.

3. What's Needed?

To enable BitLocker, ensure the following requirements and conditions are met:

- **USB drive** – Required to securely save the **BitLocker recovery key** during the encryption process. This key is needed to access the system in case of lockout.
- **USB keyboard** – Required for system interaction during login and configuration steps, particularly if standard input devices are unavailable or restricted.
- **LabAdmin Administrative Credentials** – Confirm you have the local or domain admin rights.
- **Time Allocation** – Plan for the process to take several hours, depending on the total amount of data on the system.

- **System Availability** – Verify that no tests are currently in progress as operations will be interrupted.
- **Power Source** – The system must remain powered on throughout the encryption process.

4. How to Configure BitLocker on C: Drive

1. Insert a **USB keyboard** into the **Base**.
2. Exit the **TORCH Application**, press **CTRL + ALT + DEL**, and select **Sign Off**.
3. Log into the system using the **LabAdmin** account.
4. From the **Windows 10 Start Menu**, search for and open **Manage BitLocker** (see *Figure 1*).

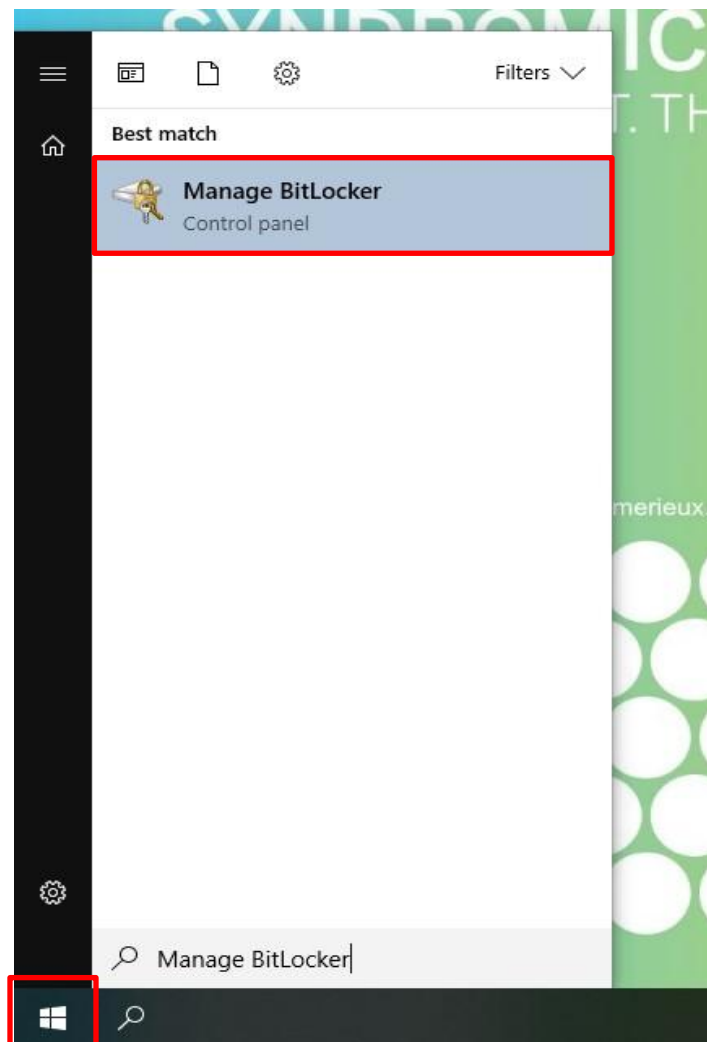


Figure 1

5. Select **Turn on BitLocker** for **C: drive**.
 - a. The **BitLocker Encryption Wizard** will appear. Follow the on-screen instructions to enable BitLocker (see *Figures 2-7*).

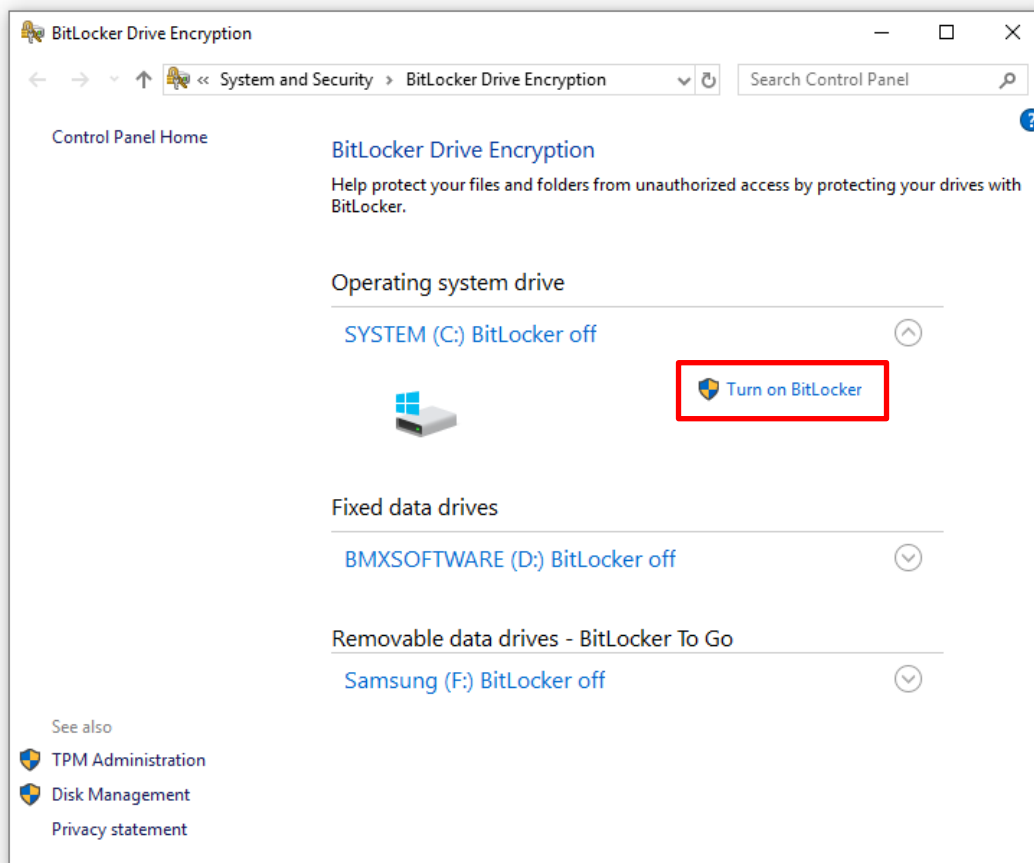


Figure 2

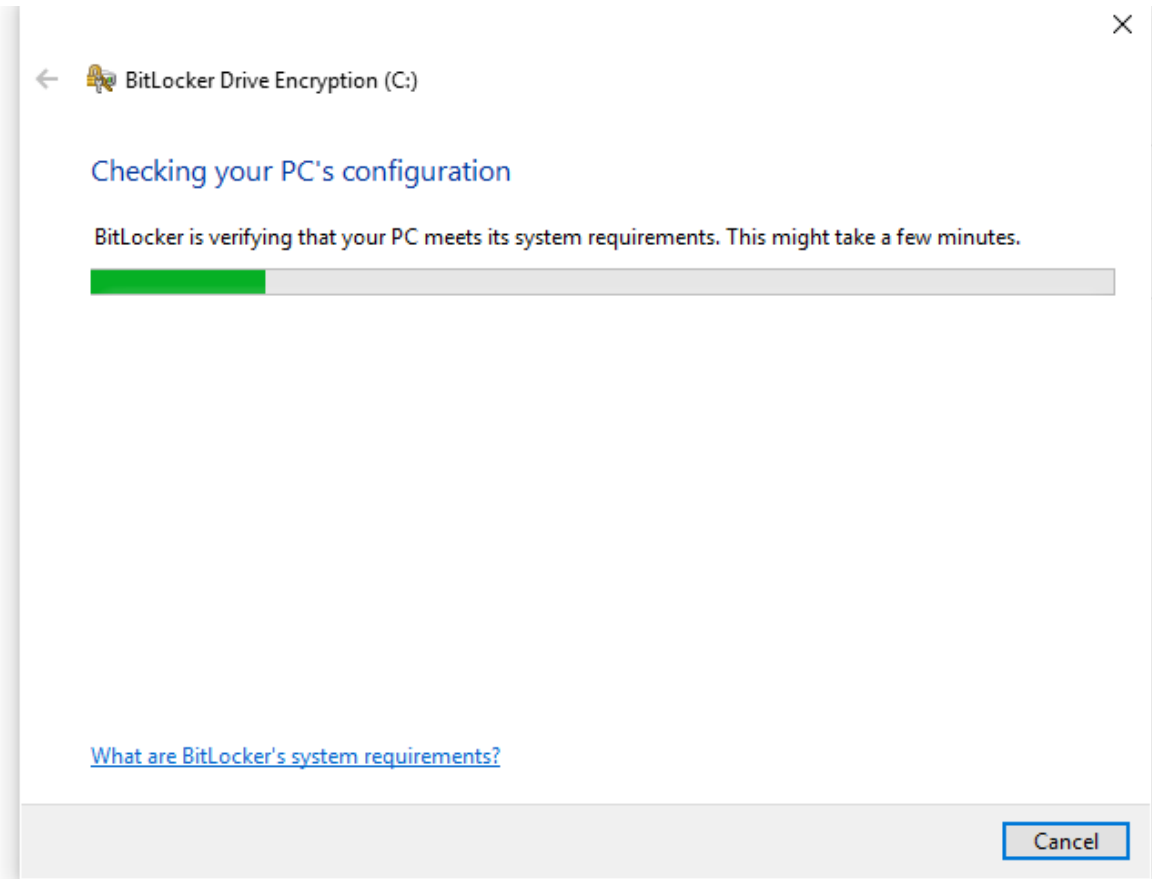


Figure 3

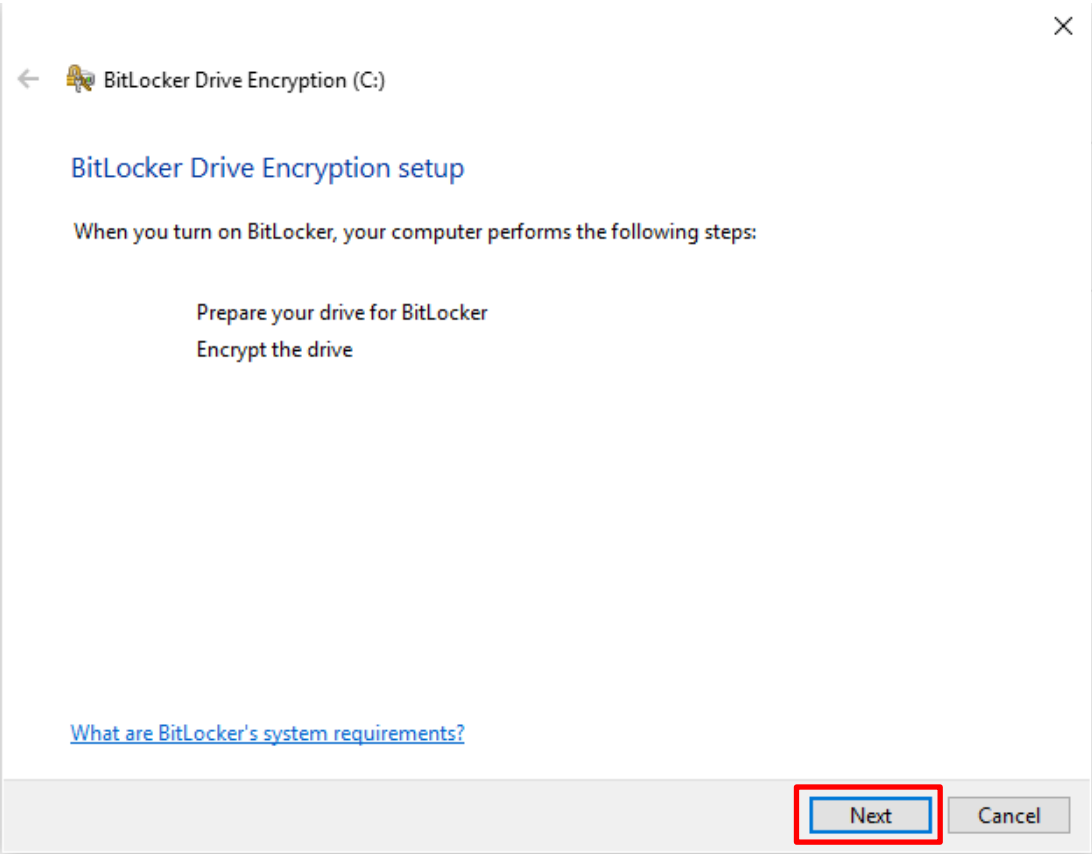


Figure 4

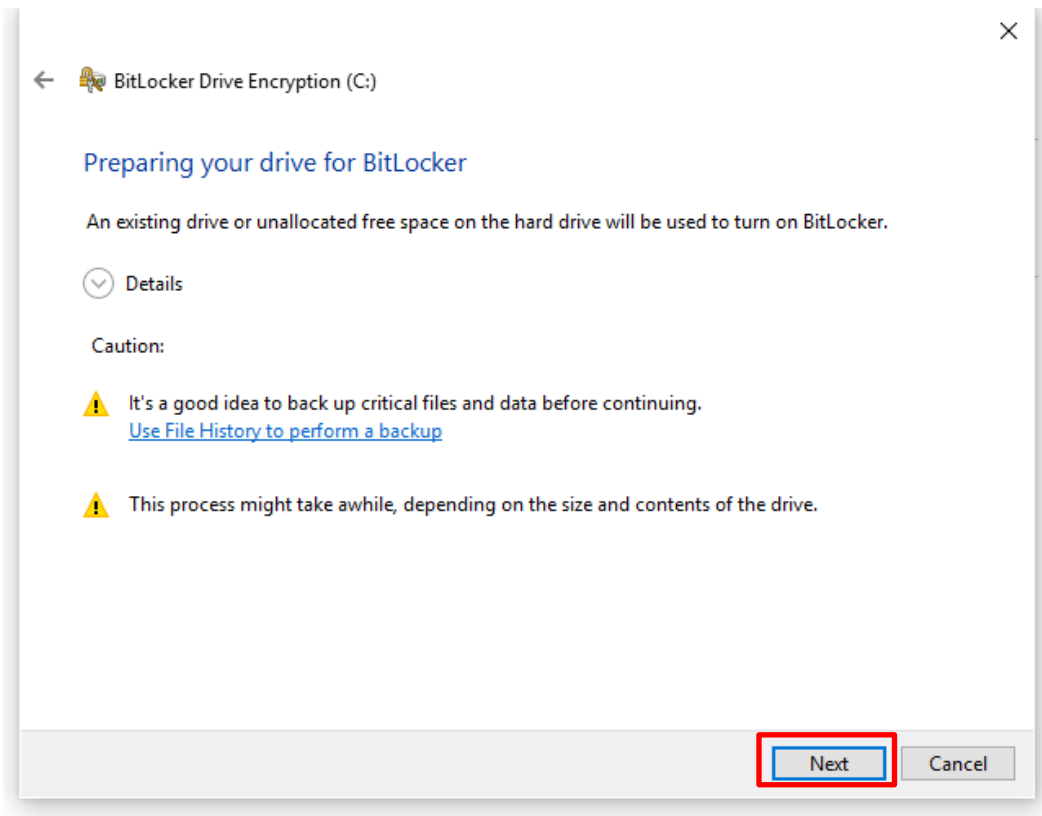


Figure 5

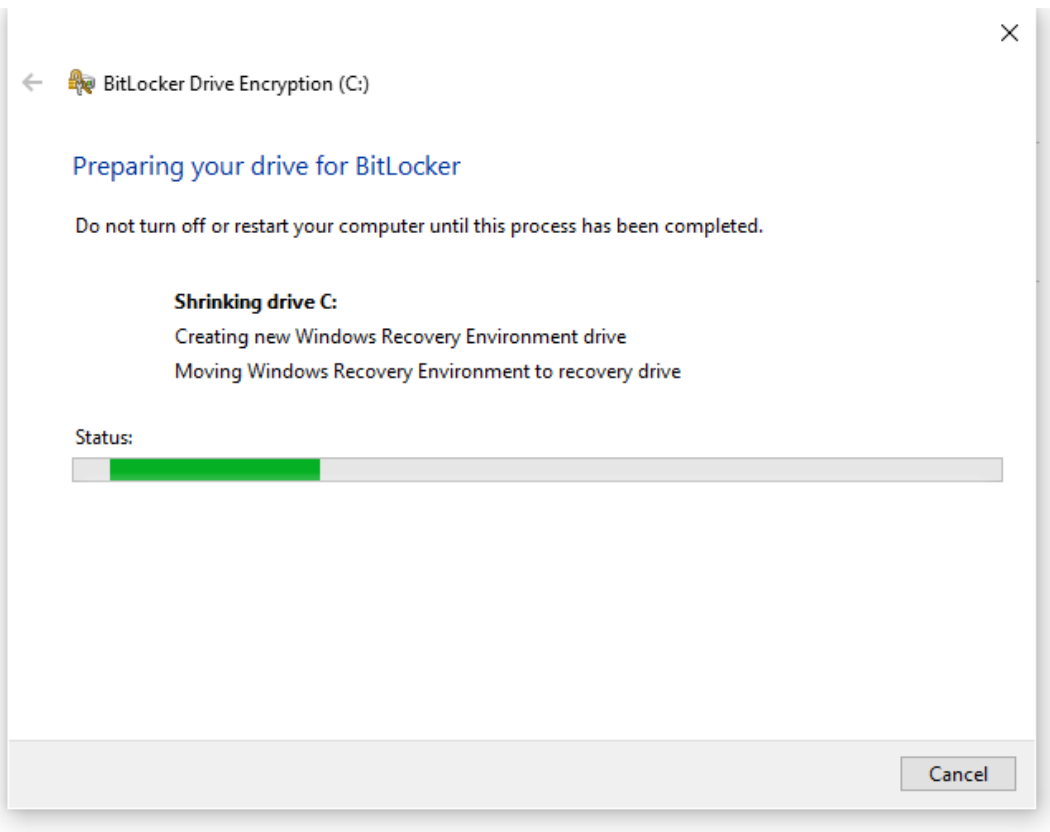


Figure 6



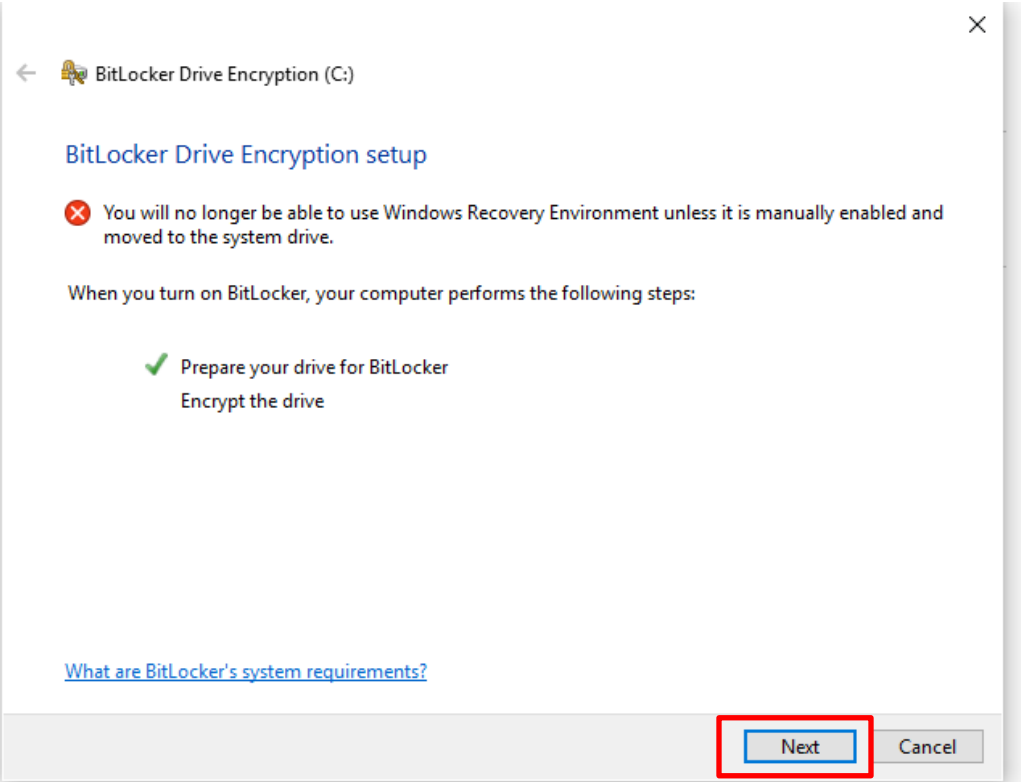


Figure 7

6. Insert the **USB drive** into the **Base**. Once connected, select **Save to a file** (see *Figure 8*).

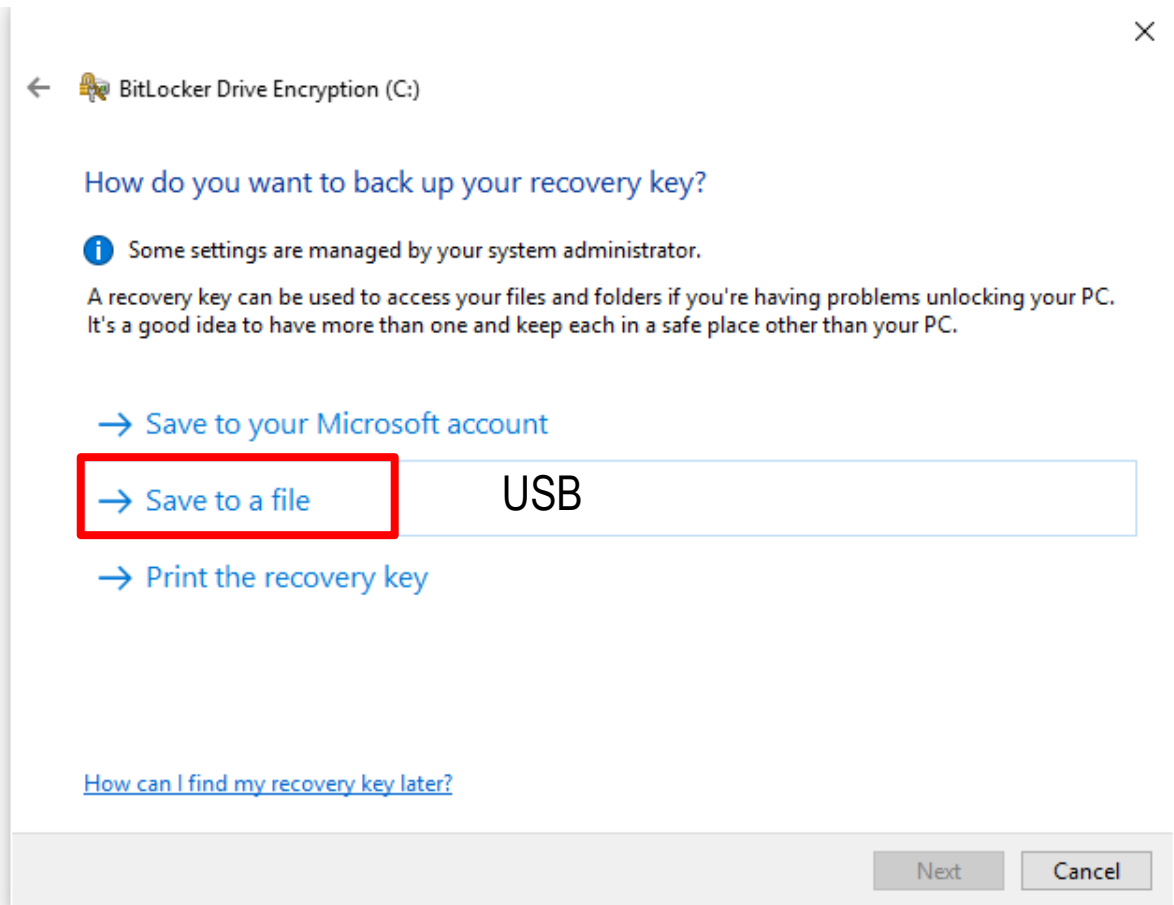
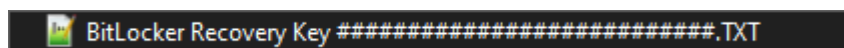


Figure 8

7. The **Windows Explorer** window will open. Select the **USB drive** you inserted to save the **BitLocker recovery key**. Ensure the USB drive is labeled and tracked.

NOTE: Once **BitLocker** is enabled, the **recovery key** becomes critical for regaining access if the system is locked. It is the **customer's responsibility** to securely store and maintain this key.



NOTE: The **BitLocker recovery key** stored on the USB drive will appear similar to the example above. The **numeric values (recovery key ID and password)** are used to unlock the system.

8. Select how much of your drive to encrypt, then select **Next** (see *Figure 9*).

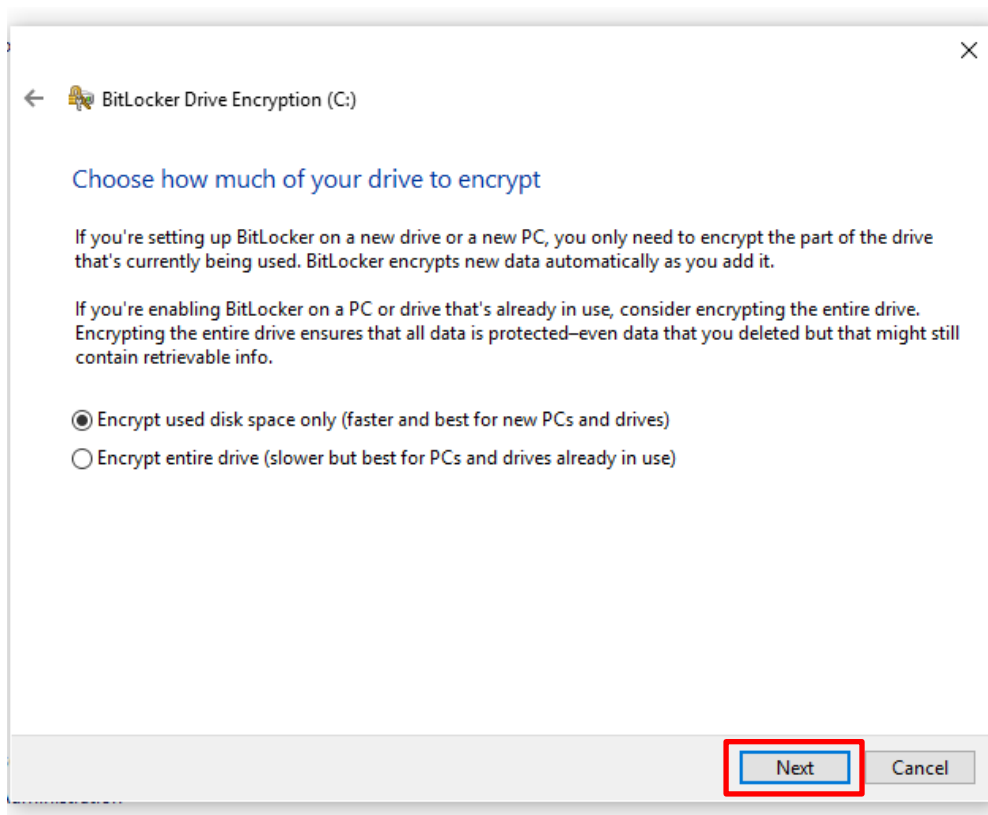


Figure 9

- a. **New system:** Select **Encrypt used disk space only**. All new data will be encrypted as it is written to the disk. This process typically takes **20-30 minutes**.
- b. **Existing system with test data:** Select **Encrypt entire drive**. All existing and new data on the drive will be encrypted. This process is expected to take **several hours**, depending on the amount of data on the drive.

9. Select **Run BitLocker system check**. Select **Continue** (see *Figure 10*).

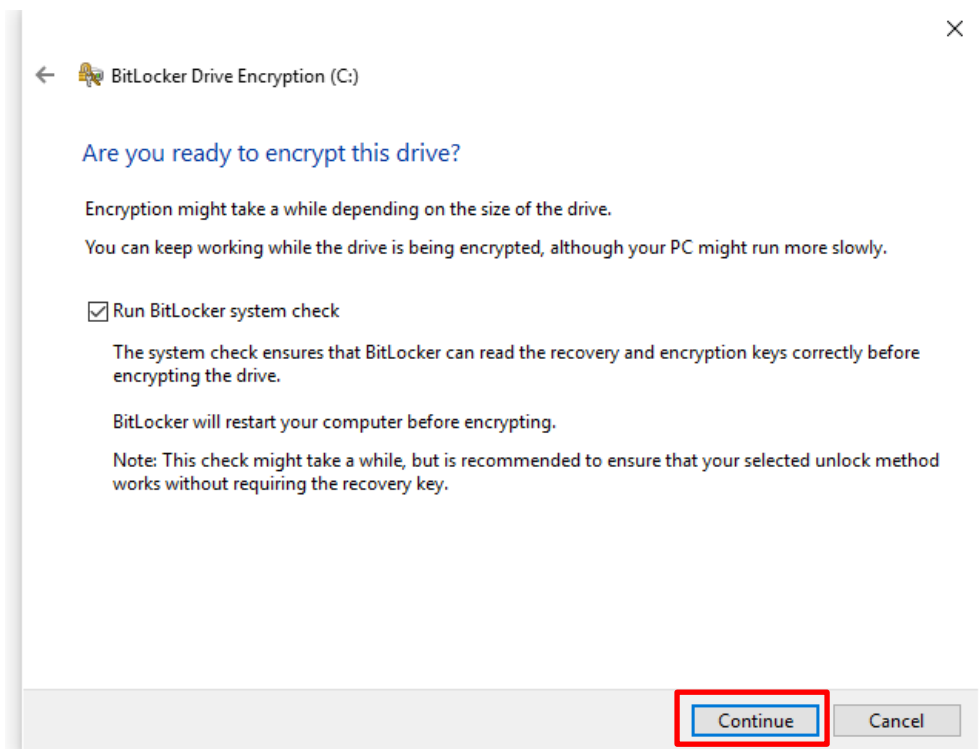


Figure 10

10. After **BitLocker encryption** is complete, restart the system to finalize setup and return to the **TORCH Software** (see *Figure 11*).

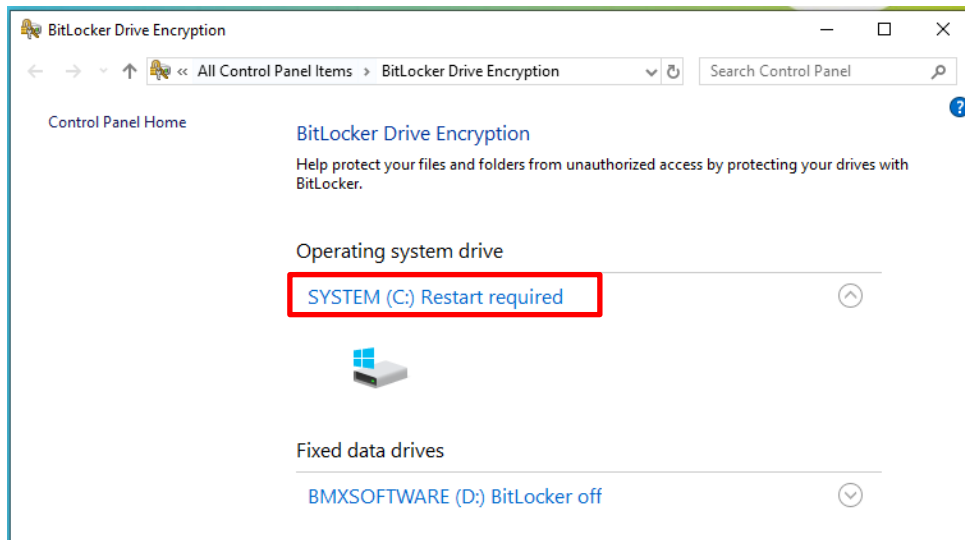


Figure 11

11. To restart the system, select **Windows Start Icon** → **Continue** → **Restart now** → **Wait for encryption to finish** (see *Figure 12*).

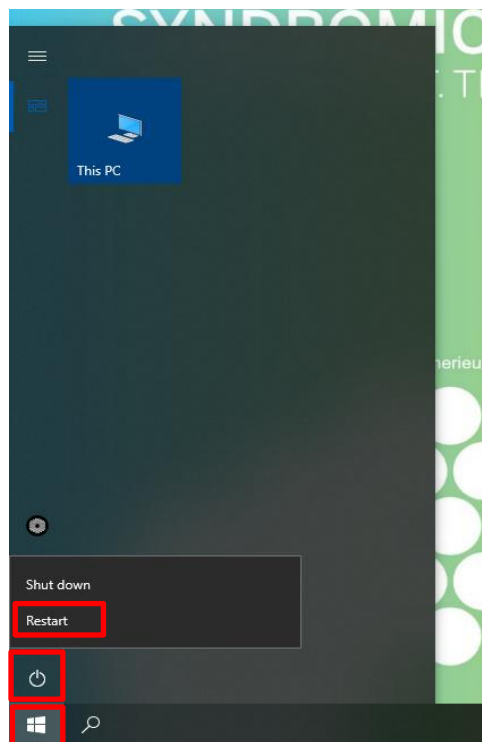


Figure 12



5. How to Configure BitLocker on D: Drive

NOTE: To encrypt the D: drive and preserve system functionality, the C: drive must also be encrypted. Ensure BitLocker encryption has been successfully completed on the C: drive before proceeding with D: drive encryption. After both drives are encrypted, the D: drive must be set to auto-unlock (see steps 14–15).

1. Insert a **USB keyboard** into the **Base**.
2. From the **TORCH Application**, press **CTRL + ALT + DEL**, then select **Sign Off**.
3. Log in using the **LabAdmin** account.
4. From the **Windows 10 Start Menu**, search for and open **Manage BitLocker** (see *Figure 13*).

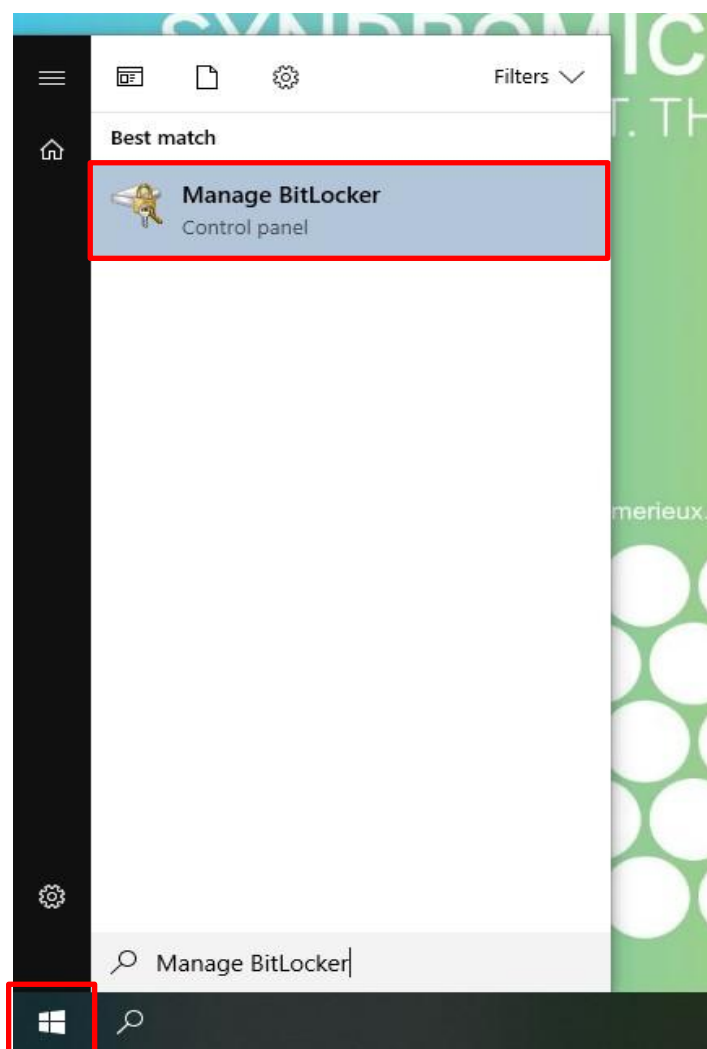


Figure 13

5. Select **Turn on BitLocker** for the **D: drive** (see *Figure 14*).

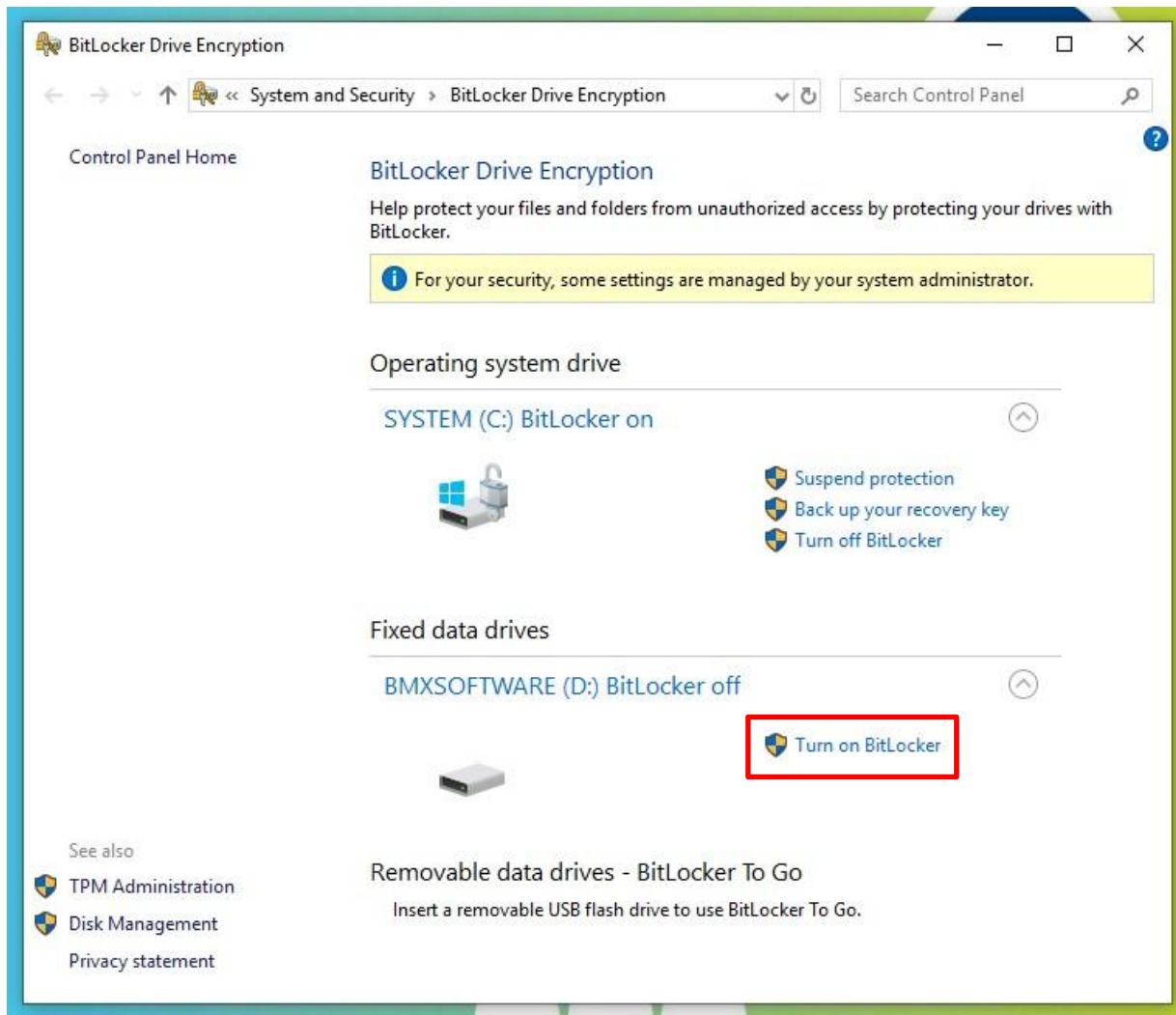
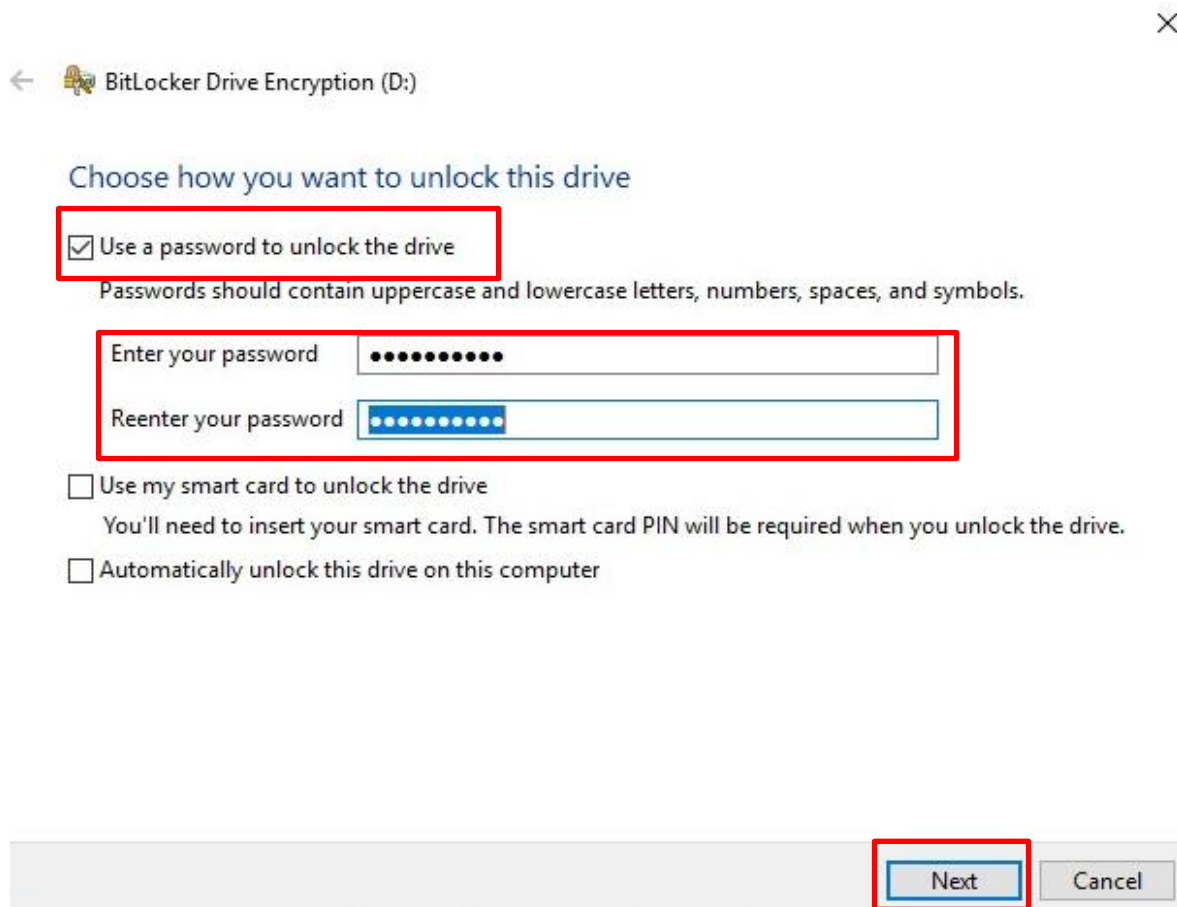


Figure 14

- Choose how you want to unlock the **D: drive** by selecting “**Use a password to unlock the drive**,” then enter a password and select **Next** (see *Figure 15*).



← BitLocker Drive Encryption (D:) ×

Choose how you want to unlock this drive

☒ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

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.

☐ Automatically unlock this drive on this computer

Next Cancel

Figure 15

7. Insert the **USB drive** into the **Base**. Once connected, select **Save to a USB flash drive** (see *Figure 16*).

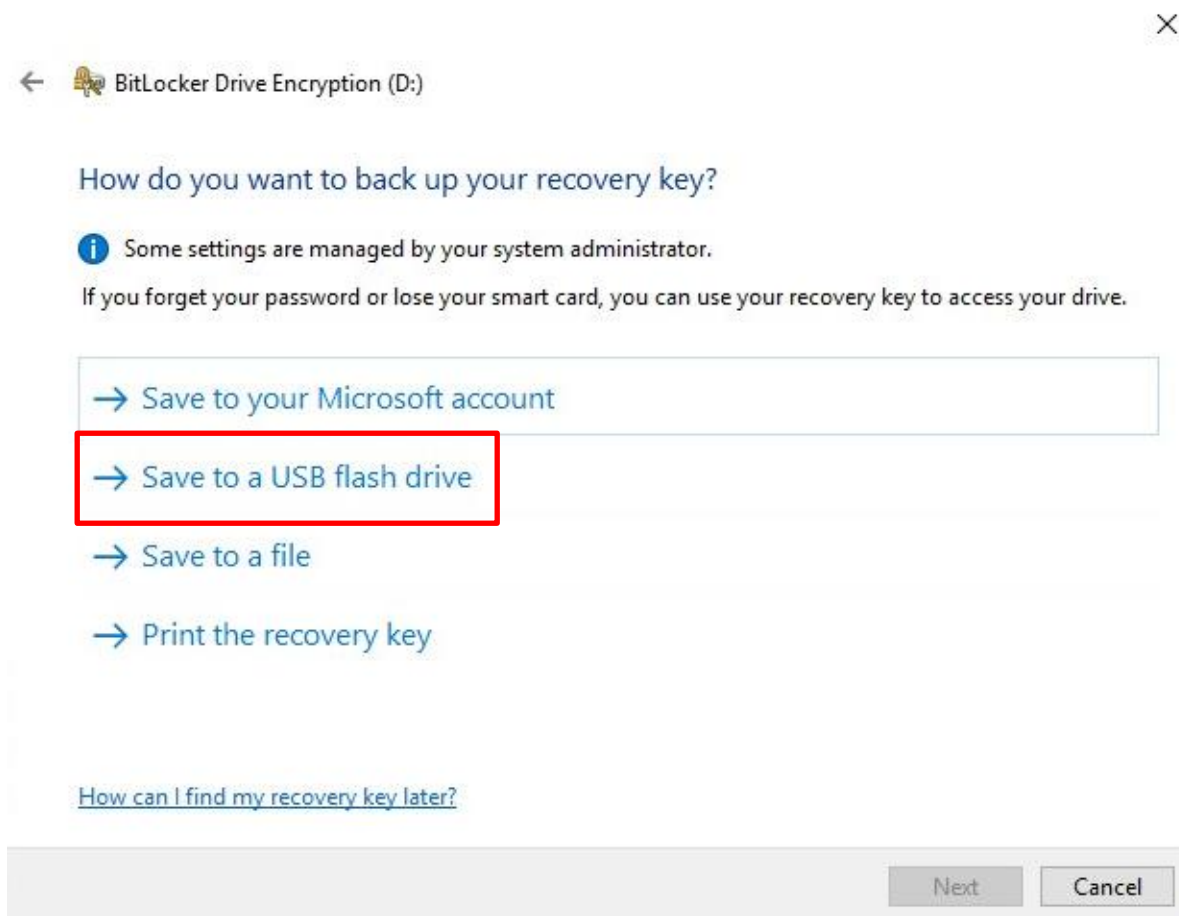
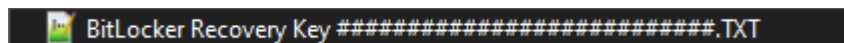


Figure 16

8. A **Windows Explorer** window will open. Select the **USB drive** you inserted to save your **BitLocker recovery key**. Ensure the USB drive is labeled and tracked.

NOTE: Once **BitLocker** is enabled, the **recovery key** becomes critical for regaining access if the system is locked. It is the **customer's responsibility** to securely store and maintain this key.



NOTE: The **BitLocker recovery key** stored on the USB drive will appear similar to the example above. The **numeric values (recovery key ID and password)** are used to unlock the system.

9. Select how much of the **D: drive** to encrypt, then select **Next** (see *Figure 17*).

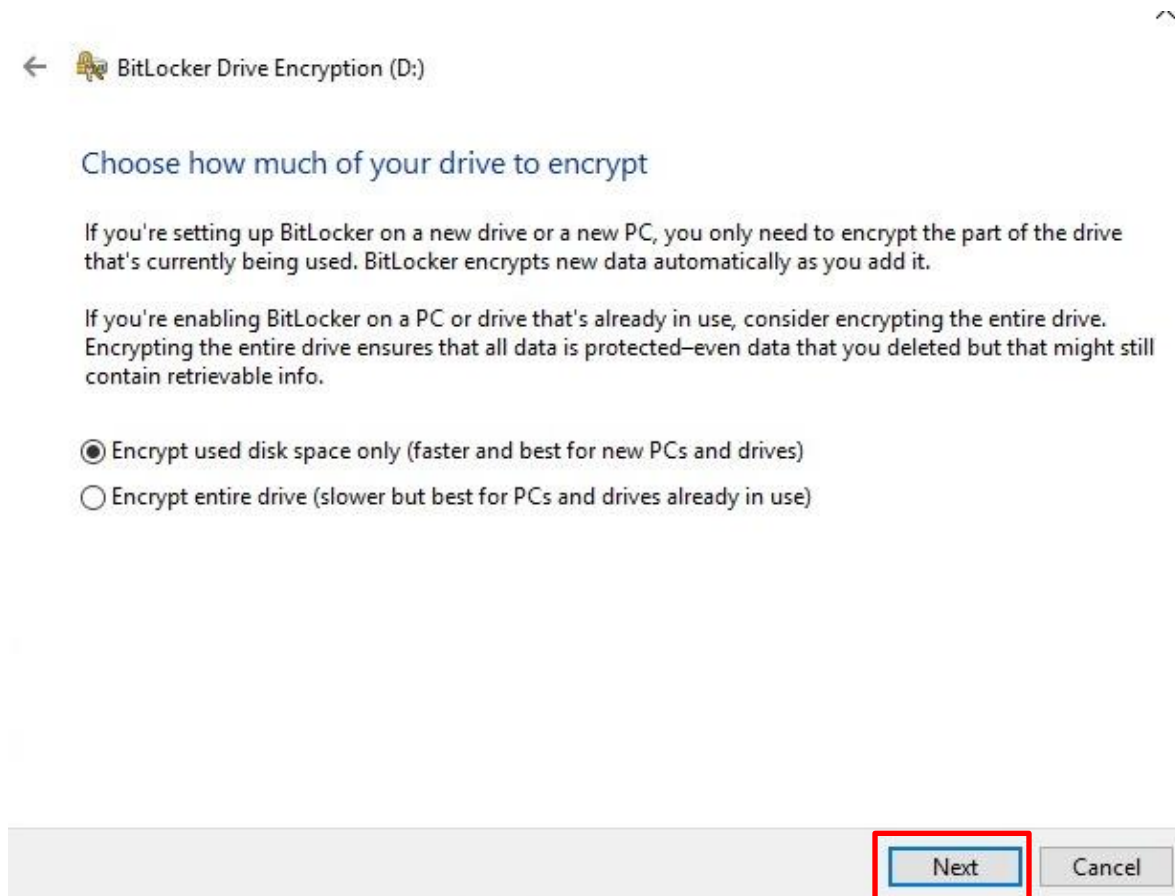


Figure 17

- a. **New system:** Select **Encrypt used disk space only**. All new data will be encrypted as it is written to the disk. This process typically takes **20-30 minutes**.
- b. **Existing system with test data** Select **Encrypt entire drive**. All existing and new data on the drive will be encrypted. This process is expected to take **several hours**, depending on the amount of data on the drive.
- c.

10. Select **Start Encrypting** for the **D: drive** (see *Figure 18*).

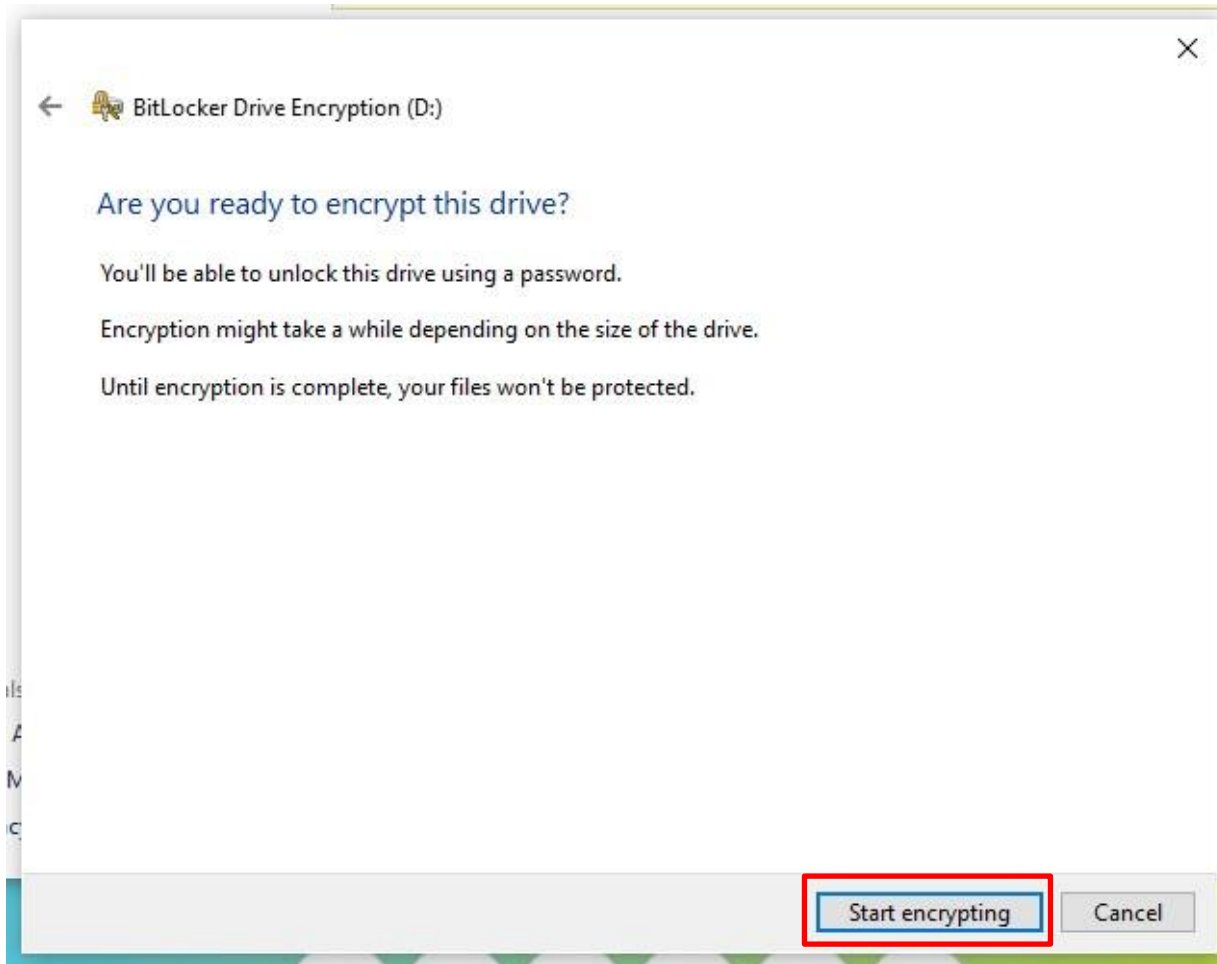


Figure 18

11. The encryption progress is displayed (see *Figure 19*).

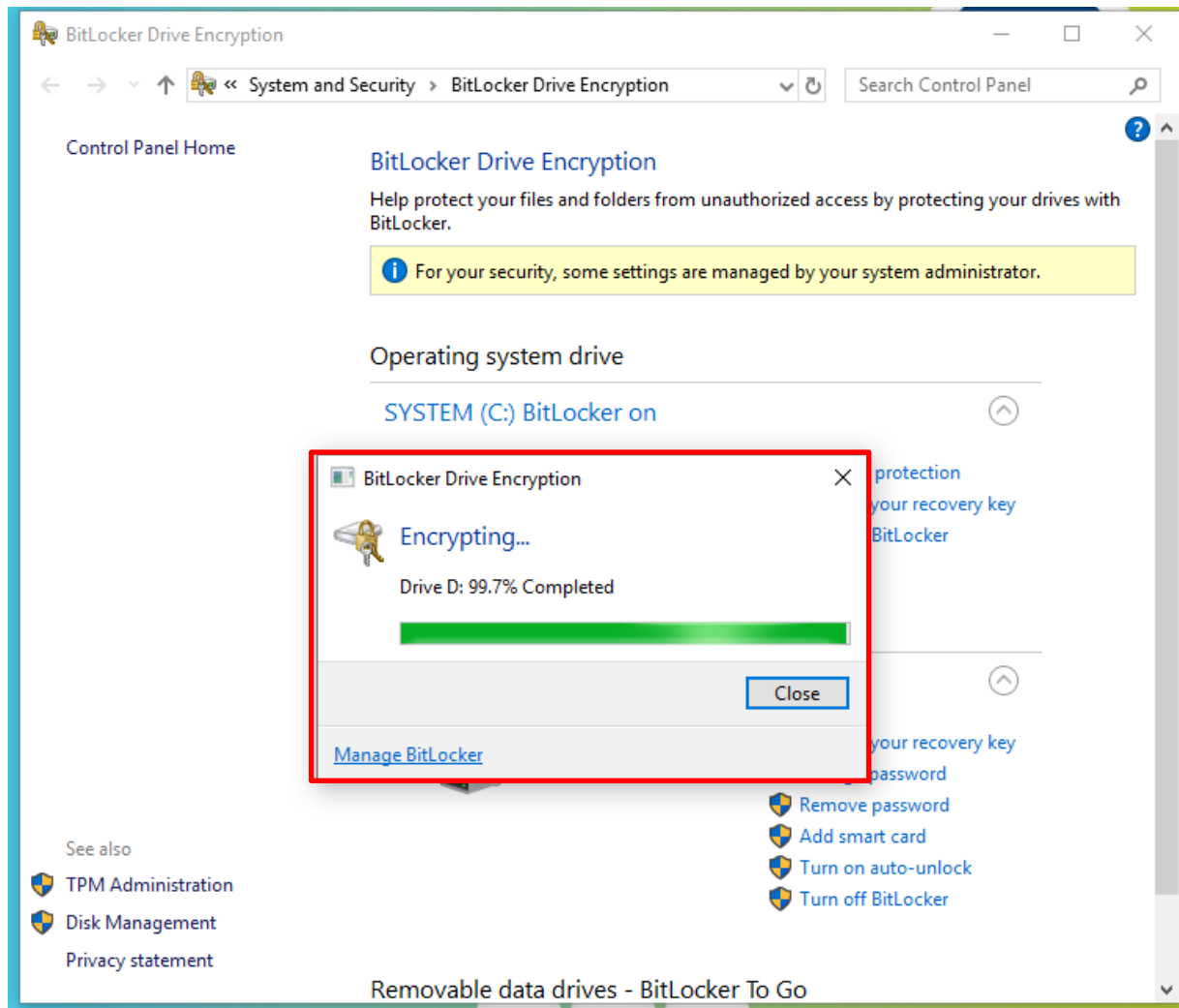


Figure 19

12. Once encryption of the **D: drive** is complete, select **Close** (see *Figure 20*).

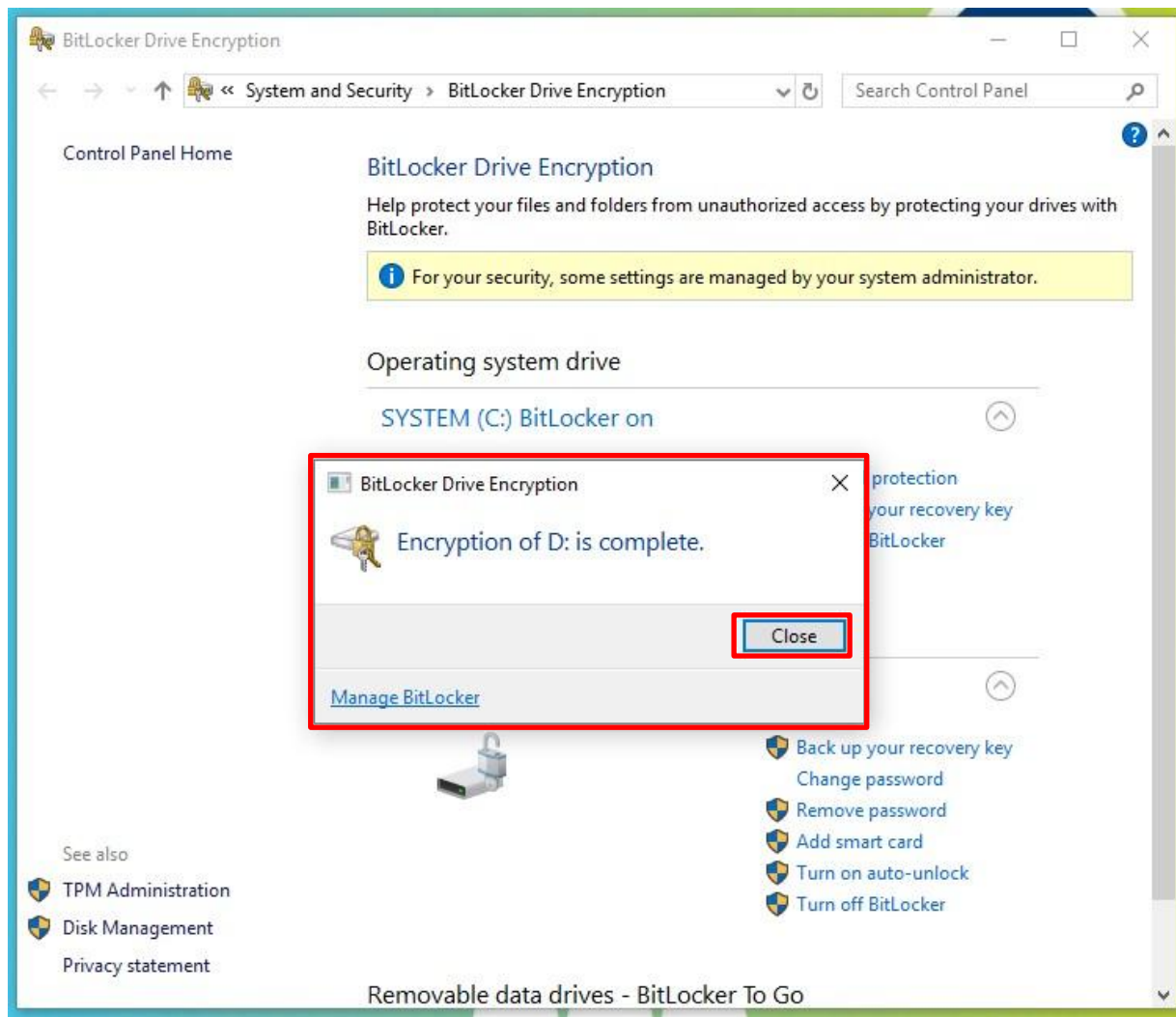


Figure 20

13. Confirmation that encryption is complete (see *Figure 21*).

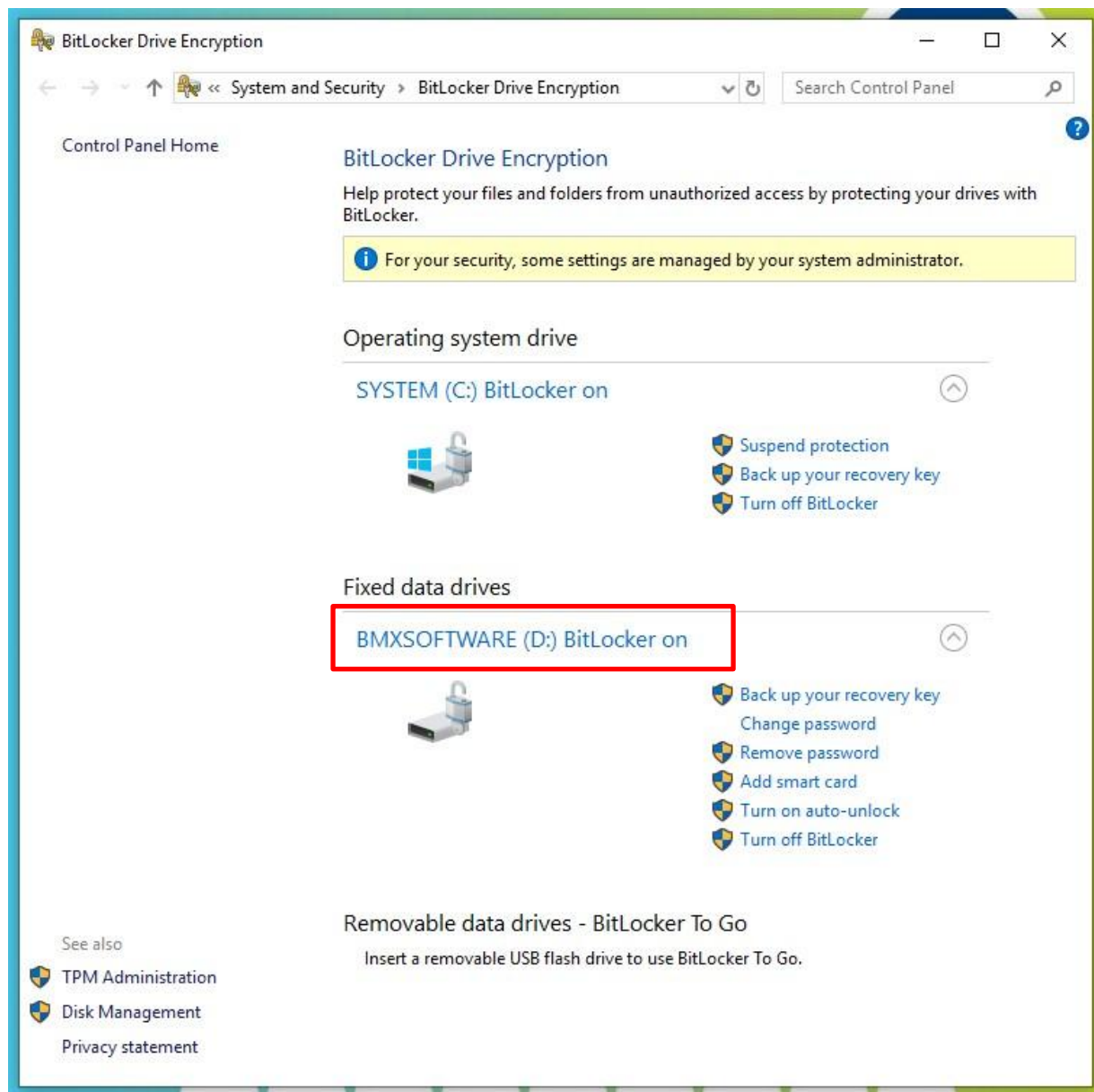


Figure 21

14. In **Manage BitLocker**, select **Turn on auto-unlock** for the **D: drive** (see *Figure 22*). Auto-unlock is required for proper system function. It lets the D: drive unlock automatically each time the system starts.

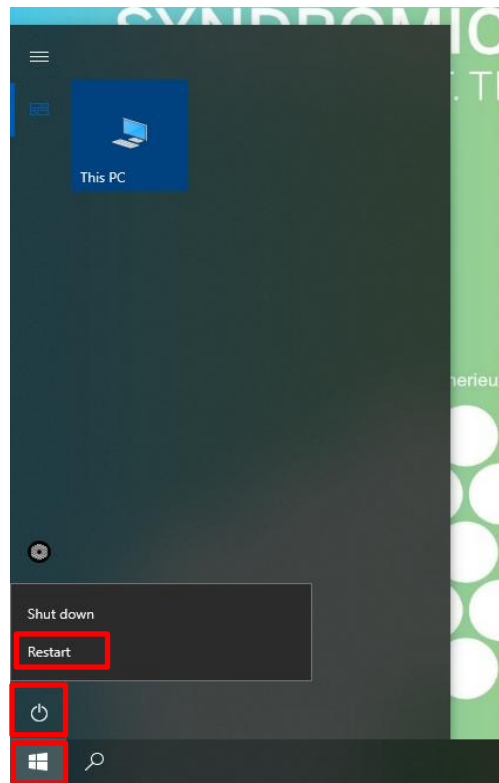


Figure 22

15. When prompted by **User Account Control**, select “**Yes**” to allow changes to the device (see *Figure 23*).

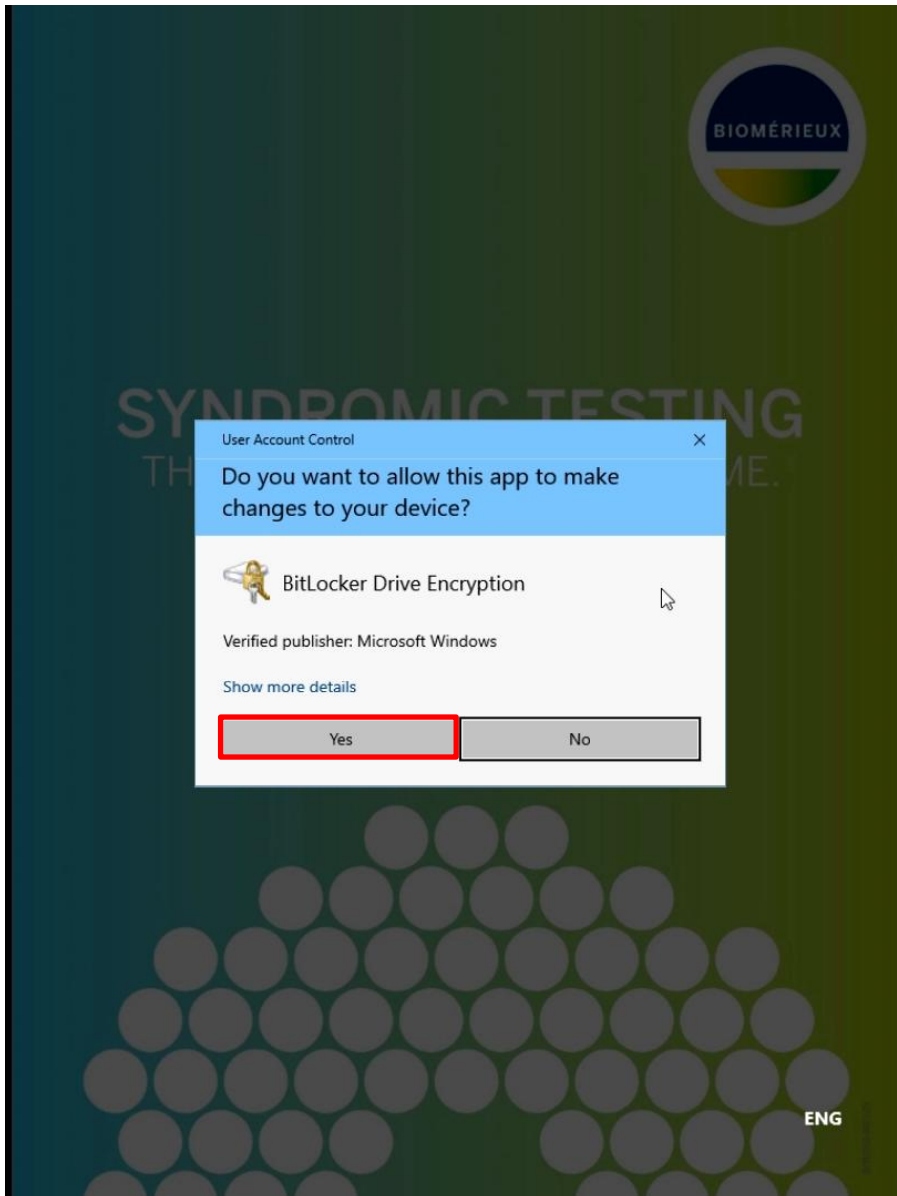


Figure 23

16. After **BitLocker encryption of the D: drive** is complete, restart the system to finalize setup and return to the **TORCH Software** by selecting the **Windows Start icon à Power à Restart** (see *Figure 24*).

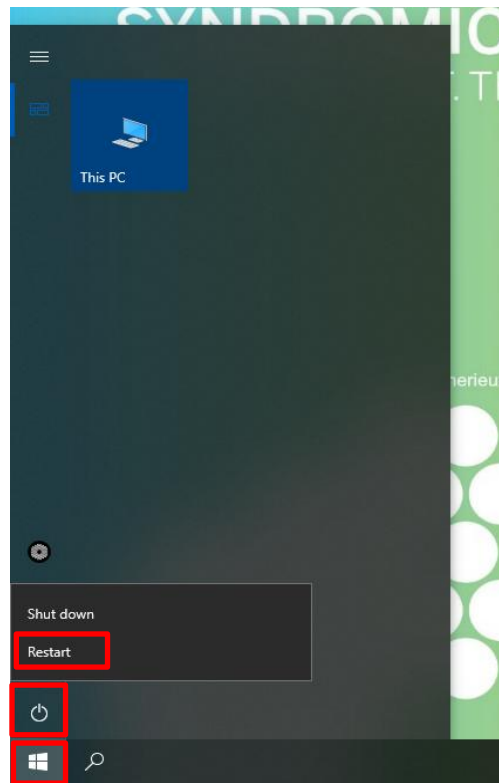


Figure 24

6. Disabling BitLocker

BitLocker must be disabled prior to sending the system for service.

NOTE: The **BitLocker Recovery Key** is **not required** to decrypt the drive.

6.1 Disabling BitLocker on C: Drive

1. Insert a **USB keyboard** into the **Base**.
2. From the **TORCH Application**, press **CTRL + ALT + DEL**, then Select **Sign Off**.
3. Log in using the **LabAdmin** account.
4. From the **Windows 10 Start Menu**, search for and open **Manage BitLocker** (see *Figure 25*).

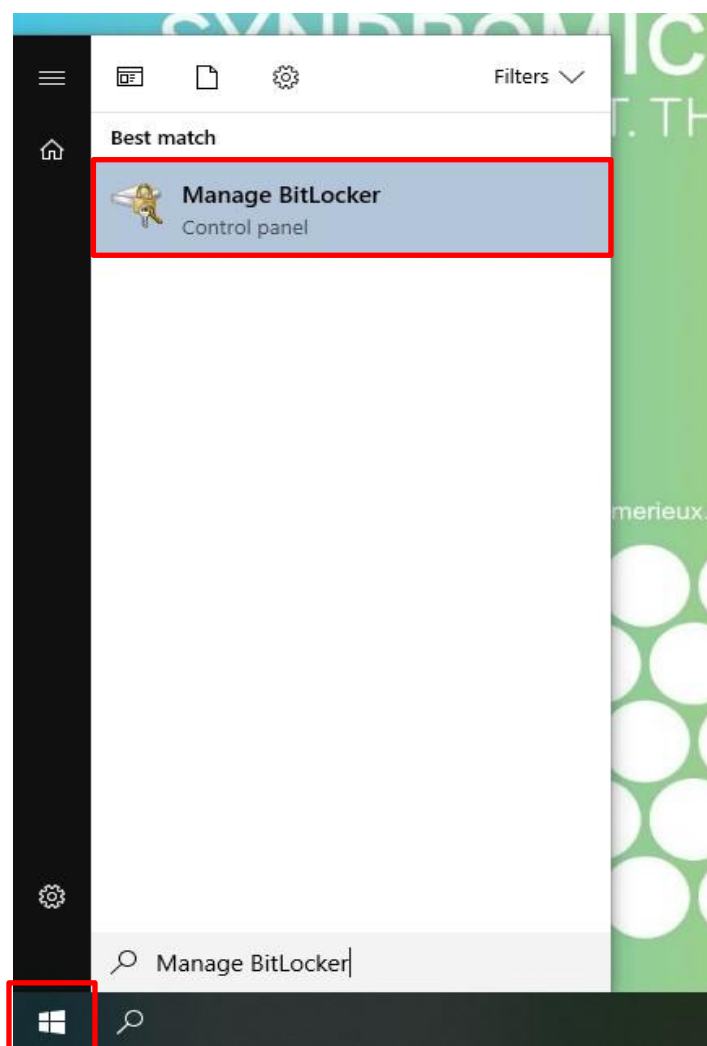


Figure 25

5. Select **Turn off BitLocker** for the **C: drive** (see *Figure 26*).

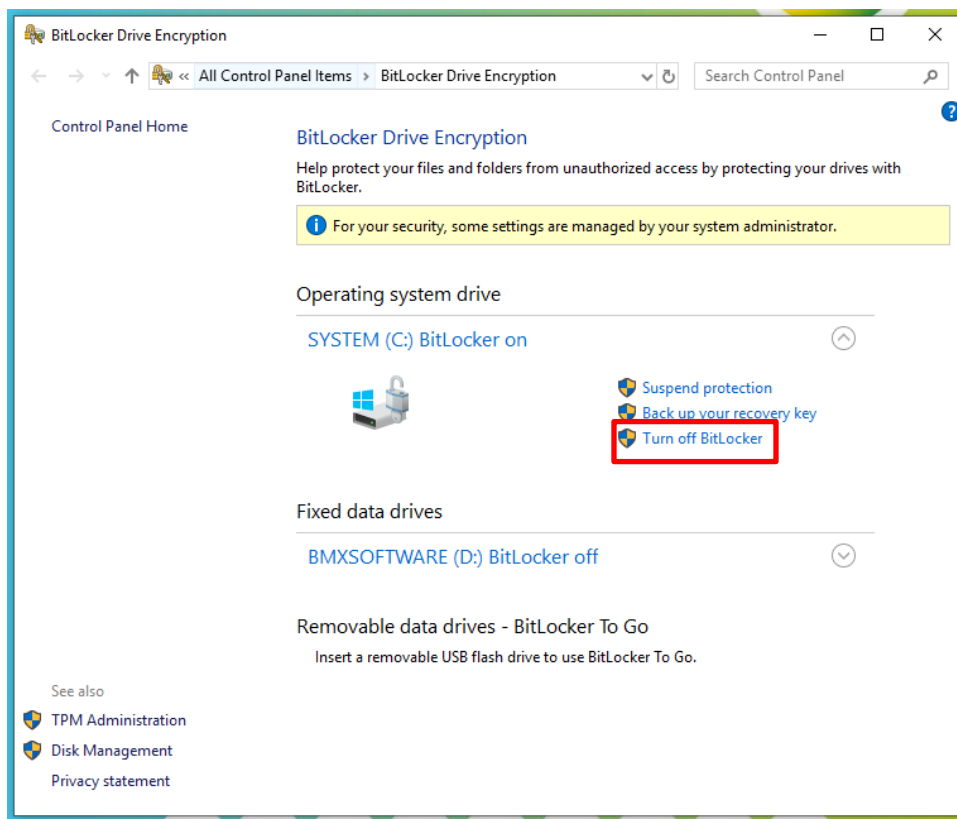


Figure 26

- When prompted, confirm that you want to **Turn off BitLocker** (see Figure 27).

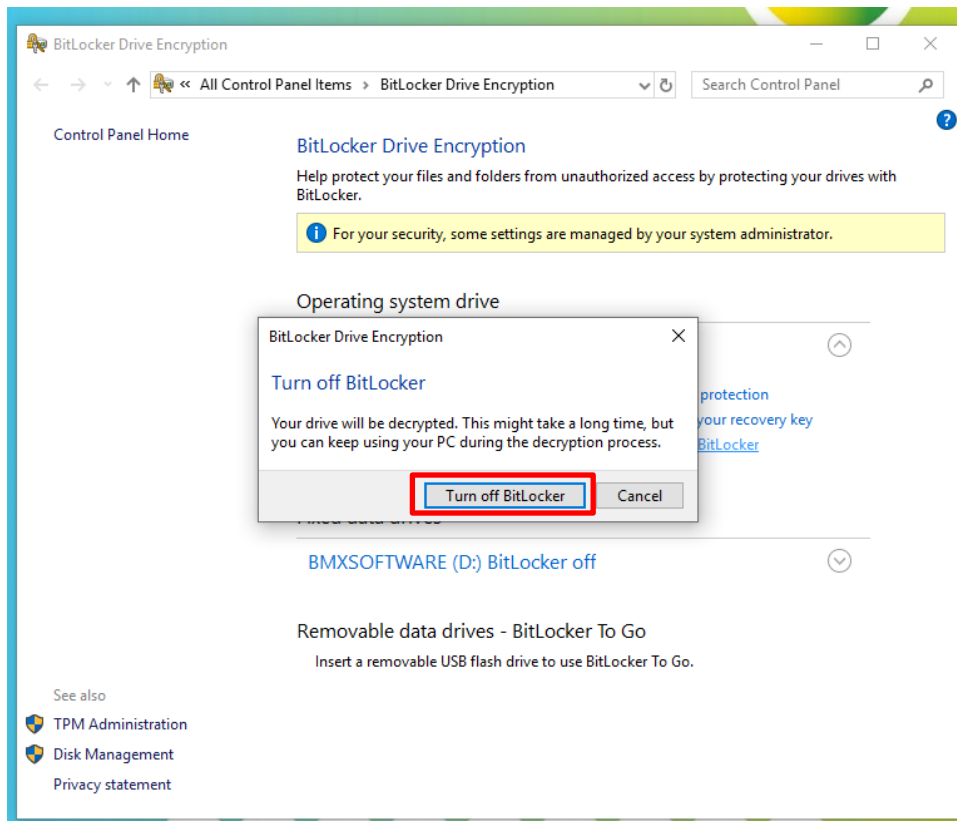


Figure 27

7. Wait for BitLocker to decrypt the **C: drive** (see *Figures 28-29*).

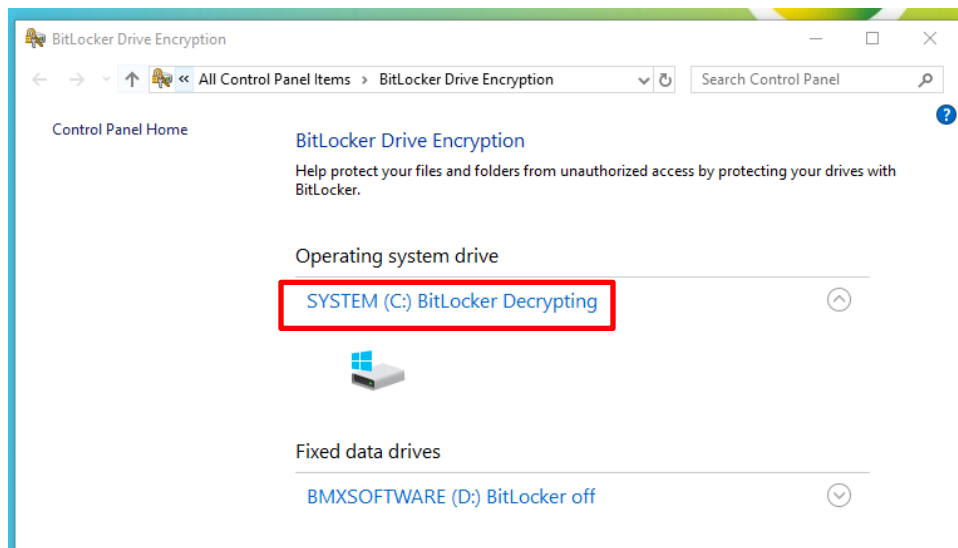


Figure 28

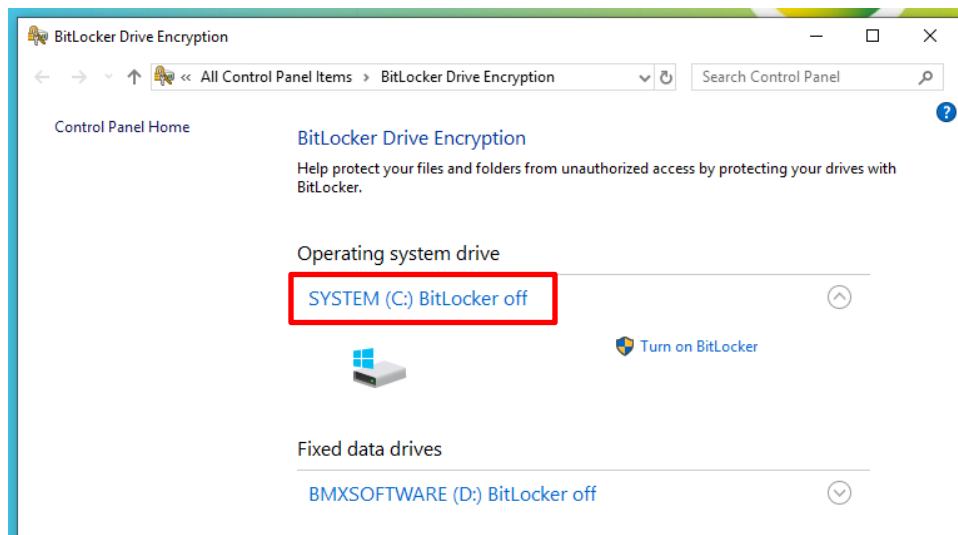


Figure 29

8. Once decryption is complete, restart the system to finalize setup and return to the **TORCH Software** by selecting **Windows Start Icon** → **Power** → **Restart** (see *Figure 30*).

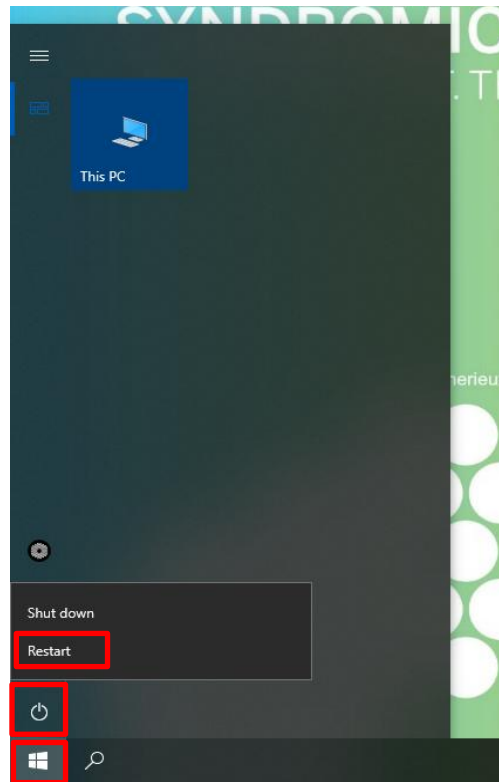


Figure 30

6.2 Disabling BitLocker on D: Drive

1. Insert a **USB keyboard** into the **Base**.
2. From the **TORCH Application**, press **CTRL + ALT + DEL**, then select **Sign Off**.
3. Log in using the **LabAdmin** account.
4. From the **Windows 10 Start Menu**, search for and open **Manage BitLocker** (see *Figure 31*).

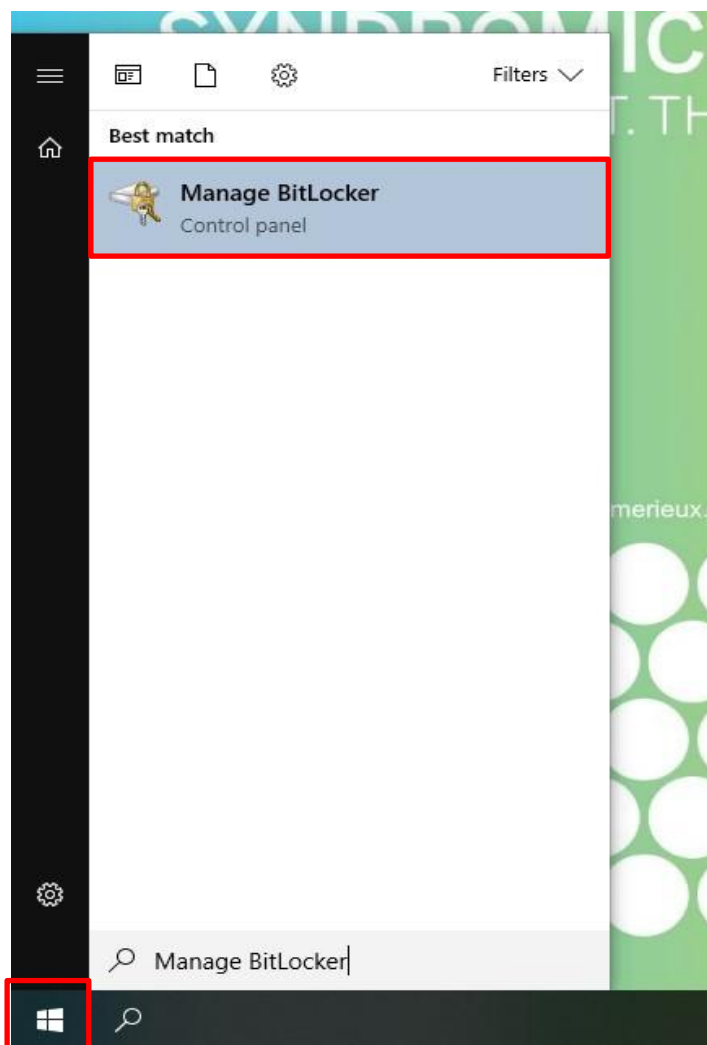


Figure 31

5. Select **Unlock drive**, enter the password, then select **Unlock** (see *Figure 32*).

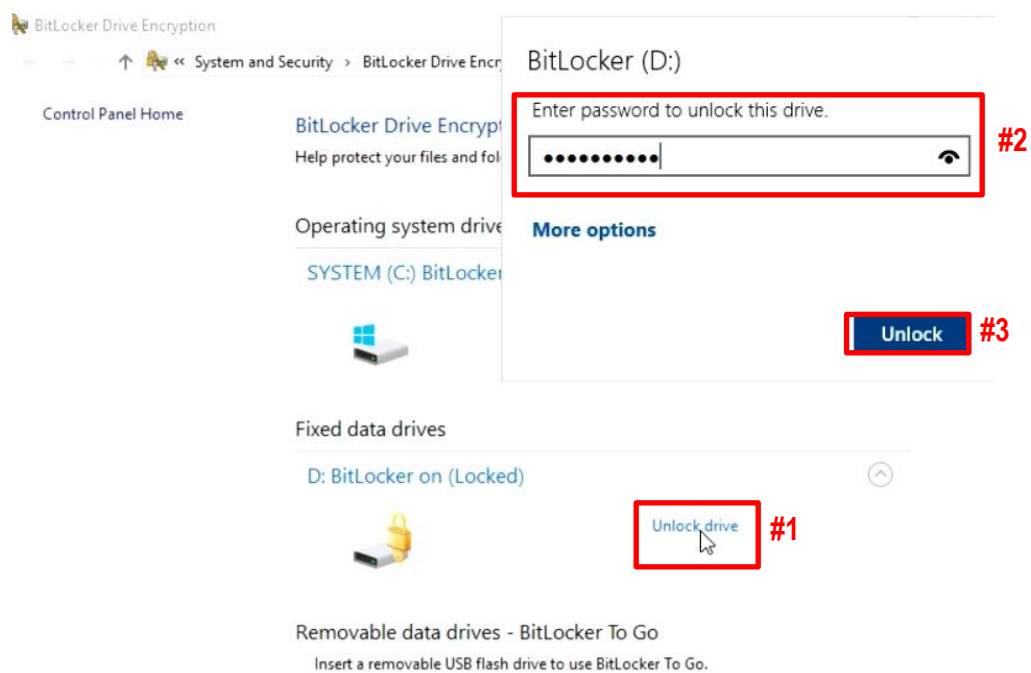


Figure 32

6. Under the **D: drive**, select **Turn off BitLocker** (see *Figure 33*).

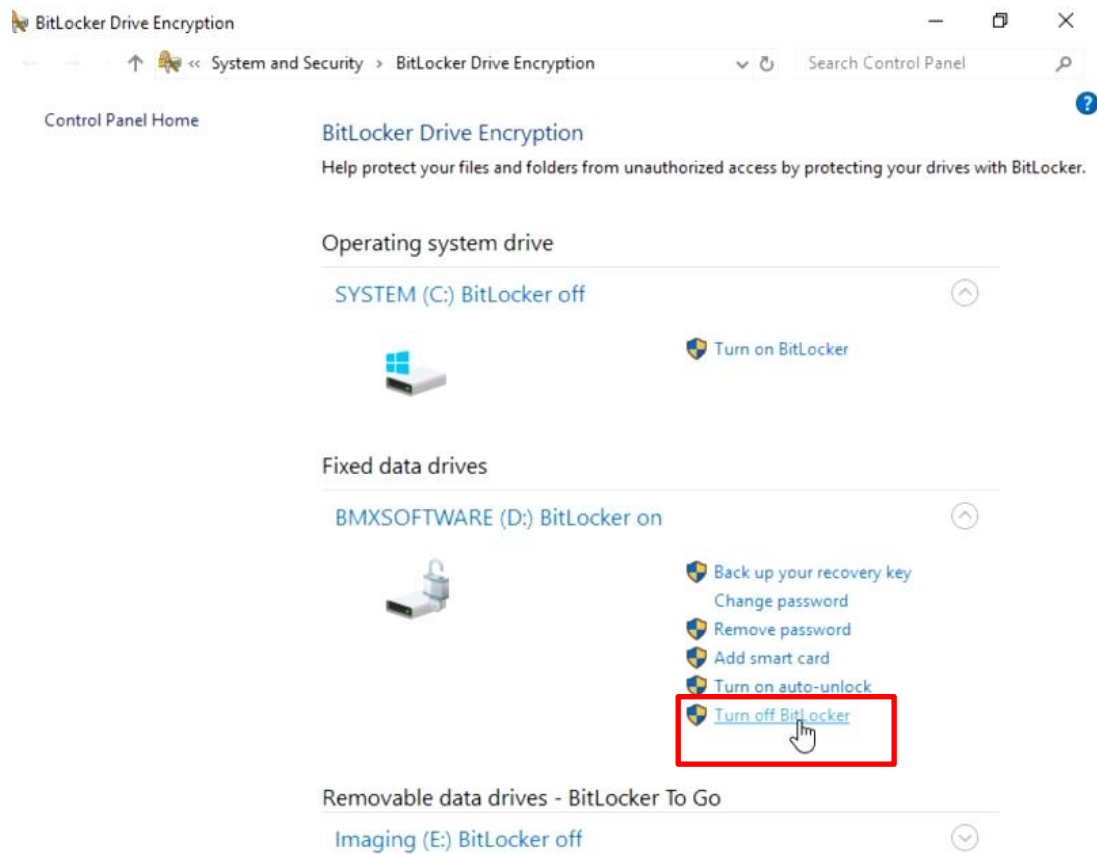


Figure 33

7. When prompted by User Account Control, select “Yes” to allow changes to the device (see *Figure 34*).

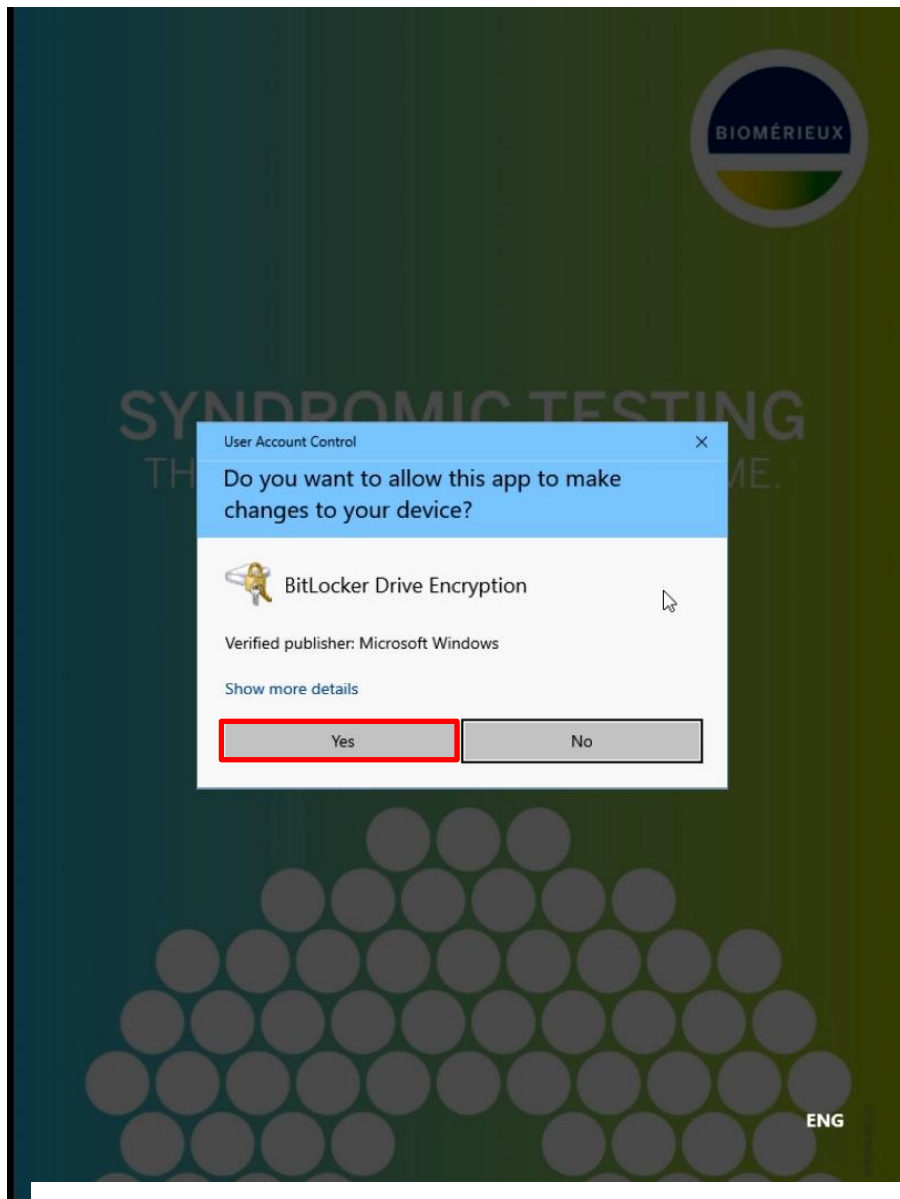


Figure 34

8. Select **Turn off BitLocker** to confirm (see *Figure 35*).

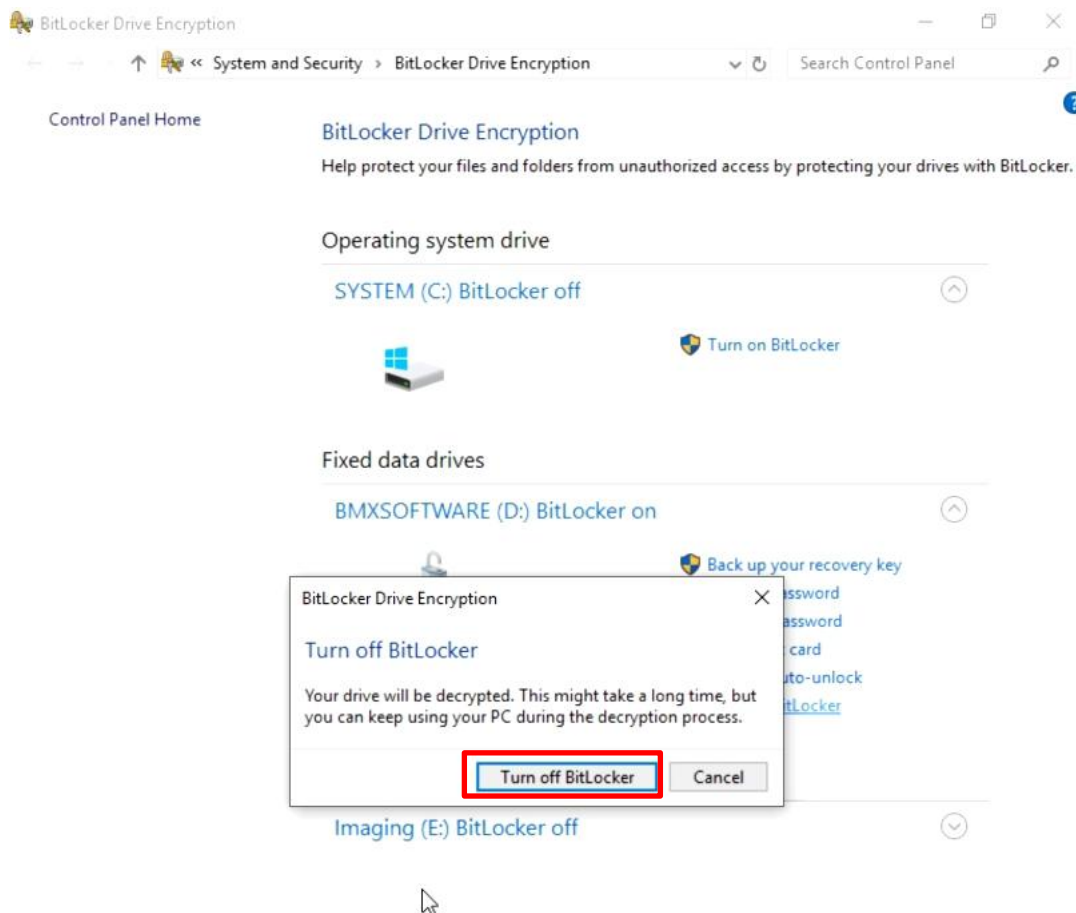


Figure 35

9. Once decryption is complete, restart the system to finalize setup and return to the **TORCH Software** by navigating to **Windows Start Icon → Power → Restart** (see *Figure 36*).

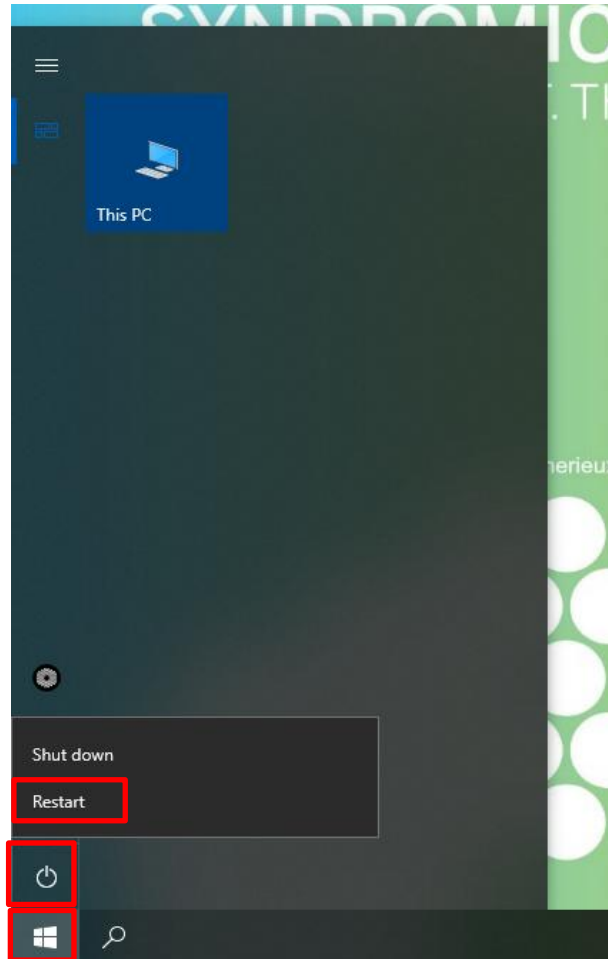


Figure 36

7. Technical Support Contact Information

bioMérieux is dedicated to providing the best customer support available. If you have questions or concerns about this process, please contact your local bioMérieux representative or your authorized distributor.

*All product names, trademarks and registered trademarks are property of their respective owners.

8. Frequently Asked Questions (FAQs)

Q: I lost the BitLocker recovery key, but I can still log in to the system. What should I do?

A: Turn off BitLocker using the steps in Section 6, then turn it back on using the steps in Sections 4 and 5. This creates a new recovery key. Save the new key to a labeled USB drive, store it securely, and give a copy to your IT department. You don't need the old recovery key to turn off BitLocker.

Q: What happens if the recovery key is lost and the system cannot be locked?

A: The encrypted drive cannot be accessed without the **BitLocker recovery key**. Contact your IT department to retrieve the copy of the recovery key they have on file. If no copy of the key can be found, the hard drive may need to be replaced with a **field replaceable unit (FRU)**.

Data loss may occur if the data was not backed up. Contact **bioMérieux Technical Support** for assistance.

9. Appendix

For additional information on BitLocker configuration and best practices, refer to the official Microsoft documentation:

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/>